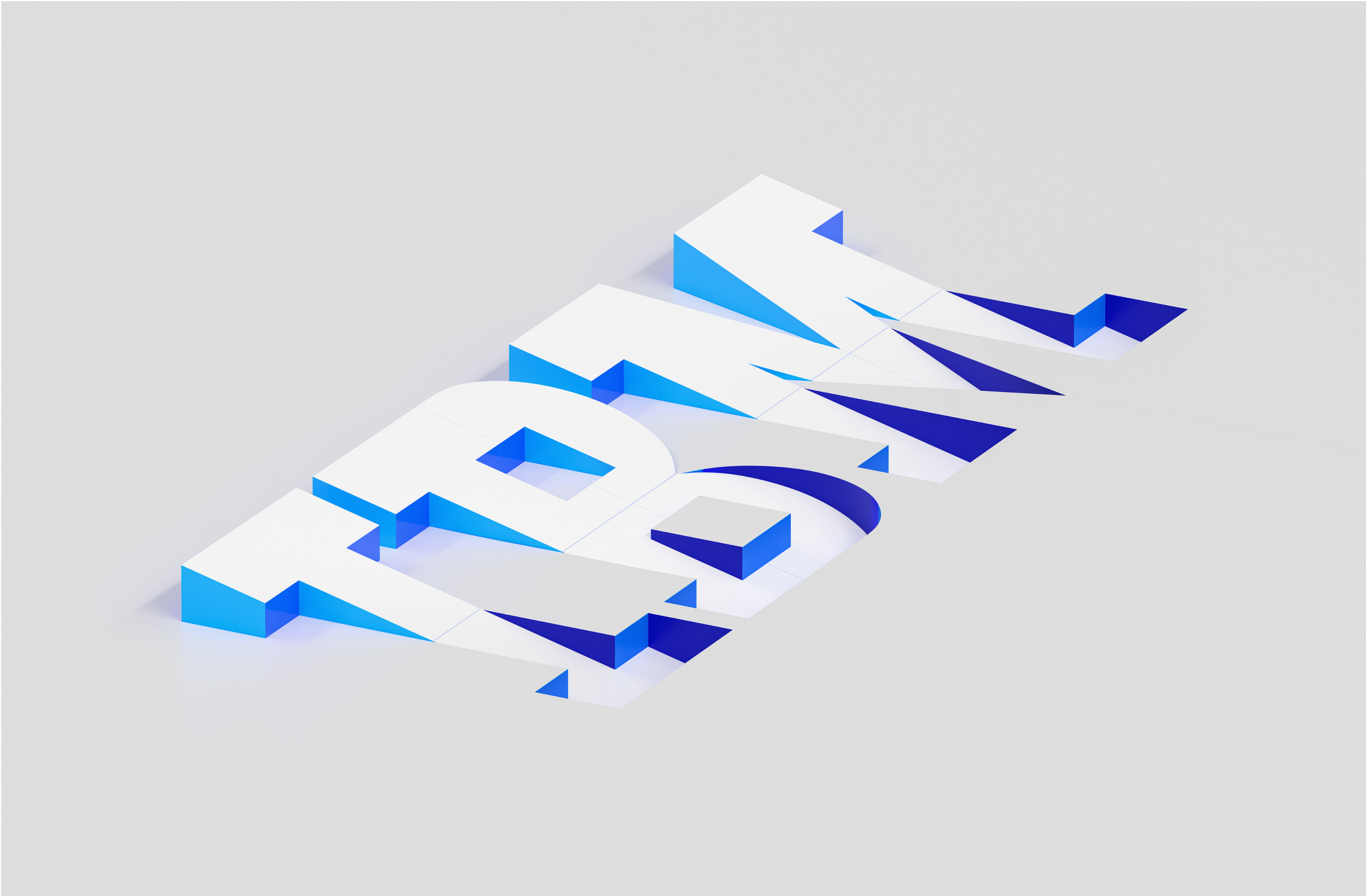


# Backup-as-a-Service for Power Virtual Server Workloads With Cobalt Iron Compass

White paper



# Edition notices

This PDF was created on 2026-05-04 as a supplement to *Backup-as-a-Service for Power Virtual Server Workloads With Cobalt Iron Compass* in the IBM Cloud docs. It might not be a complete set of information or the latest version. For the latest information, see the IBM Cloud documentation at <https://test.cloud.ibm.com/docs/pvs-baas-with-compass>.

# Backup-as-a-Service for Power Virtual Server Workloads With Cobalt Iron Compass

This white paper provides a deep dive on the fully managed secure Backup-as-a-Service (BaaS) with Cobalt Iron Compass offering in IBM Cloud for backup and recovery of AIX, Linux, IBM i, Oracle on AIX, Db2 on AIX, and SAP HANA on Linux on IBM Power Virtual Server.

## Overview

---

### IBM Power

[IBM Power](#) is a family of high-performance servers that are based on IBM Power processors. IBM Power is designed to support high-performance computing, large-scale data processing, and essential applications like ERP, CRM, and database systems. IBM Power is known for its Reliability, Availability, and Scalability (RAS), performance and sustainability.

Key features of IBM Power include:

- **Reliability:** According to [ITIC 2024 reliability survey](#), it was the 16th consecutive year that the IBM Z and IBM Power Systems have dominated with the best across-the-board uptime reliability ratings among 18 mainstream distributions. IBM Power got 99.9999% or greater availability rating.
- **Security:** Protects data and applications with built-in on-chip crypto engines and security features.
- **Performance:** Optimized for high-performance computing with advanced multi-threading capabilities.
- **Virtualization:** Supports multiple operating systems and workloads on a single machine, enhancing resource utilization.
- **AI and Machine Learning:** Suited for AI workloads with in-core Matrix Math Accelerator (MMA) accelerator, large memory capacity, and high parallelism, enabling high throughput and low latency.
- **Sustainability:** reduces environmental impact through energy efficiency, workload virtualization, optimized performance, and responsible lifecycle management.

IBM Power systems are widely used in industries such as finance, healthcare, and telecommunications for mission-critical applications.

### IBM Power Virtual Server

[IBM® Power® Virtual Server \(PowerVS\)](#) is an IBM Power server Infrastructure-as-a-Service (IaaS) offering in IBM Cloud. Power Virtual Server resources reside in IBM data centers with separate networks and direct-attached storage. The internal networks are fenced but offer connectivity options to IBM Cloud infrastructure or private cloud environments. This infrastructure design enables Power Virtual Server to maintain key enterprise software certification and support as the Power Virtual Server architecture is identical to certified private cloud infrastructure.

Besides the benefits of IBM Power, here are some added features of IBM Power Virtual Server:

- **Flexibility and scalability:** IBM Power Virtual Server, also known as a logical partition (LPAR), can be provisioned in minutes in IBM data centers or in client locations around the globe, with scalable resources adjustable based on demand.
- **Cost-effective OPEX model:** The pay-as-you-go pricing model allows for flexible billing, helping companies manage costs by only paying for the resources they use. This also provides clients with the flexibility to deploy workloads wherever they are most needed—whether on-premises for greater control and compliance or in the cloud for scalability and agility.
- **Security and reliability:** Besides the security features of IBM Power, IBM Power Virtual Server is Financial Services Validated in IBM Cloud.
- **Smooth transition to cloud:** IBM Power Virtual Server has the same architecture in a cloud or private cloud environment as IBM Power on-premises. It supports AIX, IBM i, Linux and OpenShift, and is certified for SAP and Oracle workloads, allowing a smooth transition for businesses already using IBM Power systems to cloud.
- **Seamless hybrid cloud integration:** It enables seamless integration with on-premises Power environments and cloud ecosystems, allowing businesses to expand their IT resources into the cloud without extensive reconfiguration, making it ideal for hybrid cloud strategies.

## Addressing client needs

### Need for business continuity

Enterprises are undertaking digital transformation to stay competitive and meet evolving customer demands. Digital era also poses challenges to enterprises. The rise in sophisticated cyberattacks, such as ransomware and phishing, has made it harder for organizations to keep pace with threat actors who continually refine their tactics. Remote work and cloud adoption have expanded the attack surface, increasing vulnerabilities and making it more challenging to secure dispersed networks and devices. Additionally, regulatory requirements around data protection, such as GDPR and CCPA, have introduced legal complexities, as companies now must meet stringent data security and privacy standards or risk significant fines. According to the [Cost of Data Breach Report 2025](#), the global average cost of a data breach is USD 4.44 million, with average cost surged by 9% to USD 10.22 million in the US, an all-time high for any region.

Enterprises today face a variety of threats beyond cyberattacks, including natural disasters and geopolitical risks. Natural disasters—such as hurricanes, earthquakes, and floods—can disrupt business operations, damage physical assets, and lead to data loss if adequate backup and disaster recovery plans

are not in place. Geopolitical threats, such as trade conflicts, sanctions, or political instability, can impact supply chains, restrict market access, and increase regulatory burdens, affecting a company’s ability to operate efficiently in certain regions. These factors create significant business continuity challenges, pushing enterprises to develop comprehensive risk management strategies that include resilient infrastructure, diversified supply chains, and secure, geographically dispersed data backups.

Enterprises need a robust business continuity plan to ensure operations can withstand and quickly recover from disruptions, whether due to cyberattacks, natural disasters, or system failures. Secure backups play a critical role in this plan by safeguarding copies of essential data and applications that can be rapidly restored to resume normal business functions. By maintaining encrypted and regularly updated backups in separate, secure locations—such as off-site data centers or cloud storage—organizations can minimize downtime and financial impact. Secure backups ensure that, even in worst-case scenarios, enterprises have reliable access to their data, supporting business continuity and resilience in the face of unexpected events.

## Need for cloud and hybrid cloud strategy

Enterprises are increasingly embracing cloud strategies to drive agility, scalability, and cost-efficiency in their operations. The cloud journey is a phased process, often beginning with the migration of development and testing (dev/test) environments. This initial phase allows enterprises to explore cloud benefits—like flexibility, cost savings, and scalability—without impacting critical production systems. By moving dev/test workloads to the cloud, companies can quickly provision resources, experiment with configurations, and reduce hardware expenses, all while gaining cloud management experience.

Clients can use secure backups to quickly set up development and testing (dev/test) environments in the cloud, streamlining the creation of realistic testing conditions without impacting production data. By leveraging secure backups, clients can replicate their current environment, including configurations, data, and applications, allowing developers and testers to work with accurate data in a controlled, isolated setting. This approach not only saves time but also reduces costs since there’s no need to create or maintain separate infrastructure on-premises for dev/test purposes.

## Cobalt Iron Compass

---

### When to use Cobalt Iron Compass

There are various backup and migration services for IBM Power Virtual Server in IBM Cloud catalog, which you can see when you search for Power in IBM Cloud catalog. Depending on the OS on the IBM Power Virtual Server, there are also commands to back up the file system or databases, for example, mksysb to backup root volume group and RMAN to backup Oracle database on AIX. One may get confused regarding when to adopt which option.

**Cobalt Iron Compass is the only automated, secure Backup-as-a-Service (BaaS)** for Power VS workloads running AIX, Linux, and IBM i, and it is powered by IBM Storage Protect. This IBM Cloud Catalog offering is called Secure Automated Backup with Compass. It simplifies and secures the backup and recovery of AIX, Linux, IBM i, Oracle on AIX, Db2 on AIX, and SAP HANA on Linux by offering instant setup and hands-free operations from a single unified solution. Compass is the premiere data protection solution for PowerVS workloads. In addition, Compass has been deeply integrated with and optimized for the IBM Cloud.

When to use Cobalt Iron Compass:

- **Secure backup** – Clients need to protect AIX, Linux, IBM i, Oracle, Db2, or SAP workloads from on-premises to cloud or cloud to cloud, with features like Zero Access® architecture, automated operations, analytics, deduplication, encryption, ransomware detection, etc.
- **Fully managed** - Clients need a fully configured and managed BaaS solution and don’t want to spend time and resources setting up, tuning, administering, and monitoring the many components of backup systems manually (in some cases multiple systems).
- **Flexible SaaS pricing model** – Clients want pay-as-you-go pricing model and only pay for what they use.
- **Mature and scalable protection for PowerVS workloads** – Clients require robust, integrated, and highly scalable protection for PowerVS workloads that is also IBM Cloud-optimized for performance and cost reduction.
- **Data governance** – Clients require proof of and insights into data custodianship of backup data and operations to assist with audit and regulatory requirements.

### Why use Cobalt Iron Compass

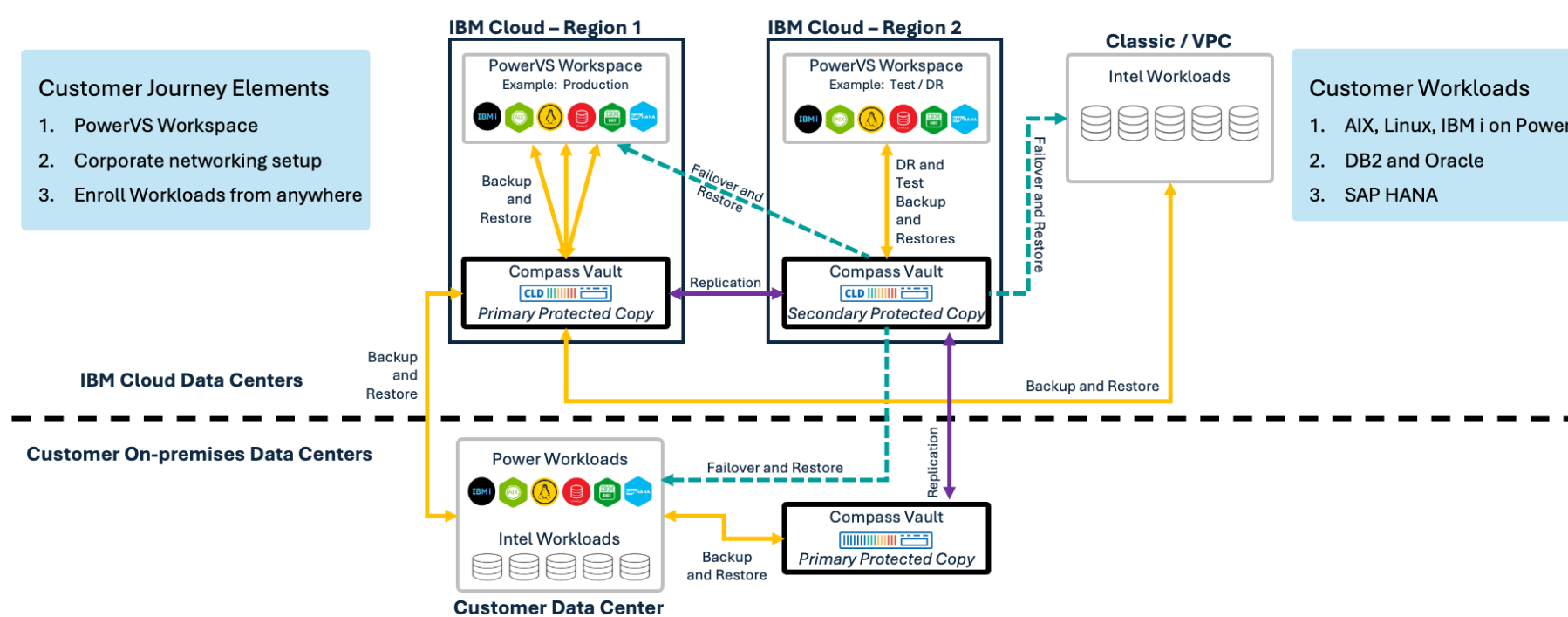
Secure Automated Backup with Compass delivers operational excellence for backup and recovery of PowerVS and other enterprise workloads. Some of the business outcomes customers can expect with Compass include the following.

- **Instant on, enterprise-class backup** – Compass provides the easy button for protecting your PowerVS and other workloads with analytics-driven automation of backup componentry and operations.
  - **Compass integration with the IBM Cloud Catalog** – Compass is preconfigured, pre-optimized, and ready to service PowerVS workloads from IBM Cloud data centers worldwide. When the BaaS service is created from the IBM Cloud Catalog, Compass integrated automation creates a Transit Gateway (if it doesn’t exist already), a backup Virtual Private Cloud (VPC), and Virtual Private Endpoints (VPEs) to securely connect the client’s PowerVS workspace and Virtual Server Instances (VSIs) with the Compass Vaults in the IBM Cloud. This automation also creates the clients’ organization in Compass along with default policies and schedules so backup operations can commence immediately.
  - **Compass Dedicated Vault options** – For customers with special capacity, performance, security, or sovereignty requirements there are also options for Dedicated Compass Vaults deployed in the client’s cloud account or on-premises at a client location.

- **Automated operations** – Ongoing backup operations are automated by Compass. Restores remain within the security control of the user and in natively integrated experiences with the application (e.g., RMAN for Oracle, Studio or Cockpit for SAP, or BRMS or SAV operations for IBM i).
- **Operational excellence with analytics-driven automation**
- **Cyber protection, detection, and analysis** – The industry-unique Compass Zero Access® architecture eliminates common cyber threat vulnerabilities in the data protection environment.
  - **Zero Access** - Compass removes access to the components of the backup infrastructure greatly reducing risk of attacks against the backup landscape.
  - **Robust encryption** - Multiple layers of encryption (client-side, in-flight, to-storage, and at-rest encryptions) remove risk of data exfiltration in backup processing.
  - **Backup data immutability** - All data ingested into Compass is immutable and inert by design, there is additive ingest only. Data is only deleted by defensible retention policies.
  - **Backup data vaulting** – Backup data is vaulted in multiple, isolated security zones.
  - **Ransomware detection** – Extensive monitoring for ransomware and DDoS (Distributed Denial of Service) indicators identifies data distortion patterns and possible cyber threats.
  - **Cyber event analytics** – Impact analysis is performed on suspicious activity to determine potentially infected systems and files, type of attack, safe recovery points, and other insights.
- **SaaS delivered with enterprise scale and maturity** – Compass modernizes enterprise backup with a SaaS delivery (whether in the cloud or on-premises), automation, analytics, and advanced security features built into the architecture (not add-ons). Compass was developed in the furnace of some of the largest backup deployments in the world (including IBM's own Office of the CIO) and is the most scalable backup product available. Compass also has deep integration with AIX, Linux, IBM i, Oracle, Db2, and SAP HANA.
- **Data Custodianship** – Compass monitors and tracks all aspects and metrics of backup operations providing robust data governance, audit readiness, and compliance assistance.
- **Consolidated management** – Compass provides a single, multi-tenant or single tenant, backup experience across IBM PowerVS cloud workloads, other cloud workloads (Alibaba, AWS, Azure, Google, and IBM Clouds), remote sites, on-premises data centers, etc. Compass enables consistent policy management, operational visibility, and reporting across all these environments, world-wide.

The following figure shows an overview of the data protection and resilience provided by the Secure Automated Backup with Compass solution.

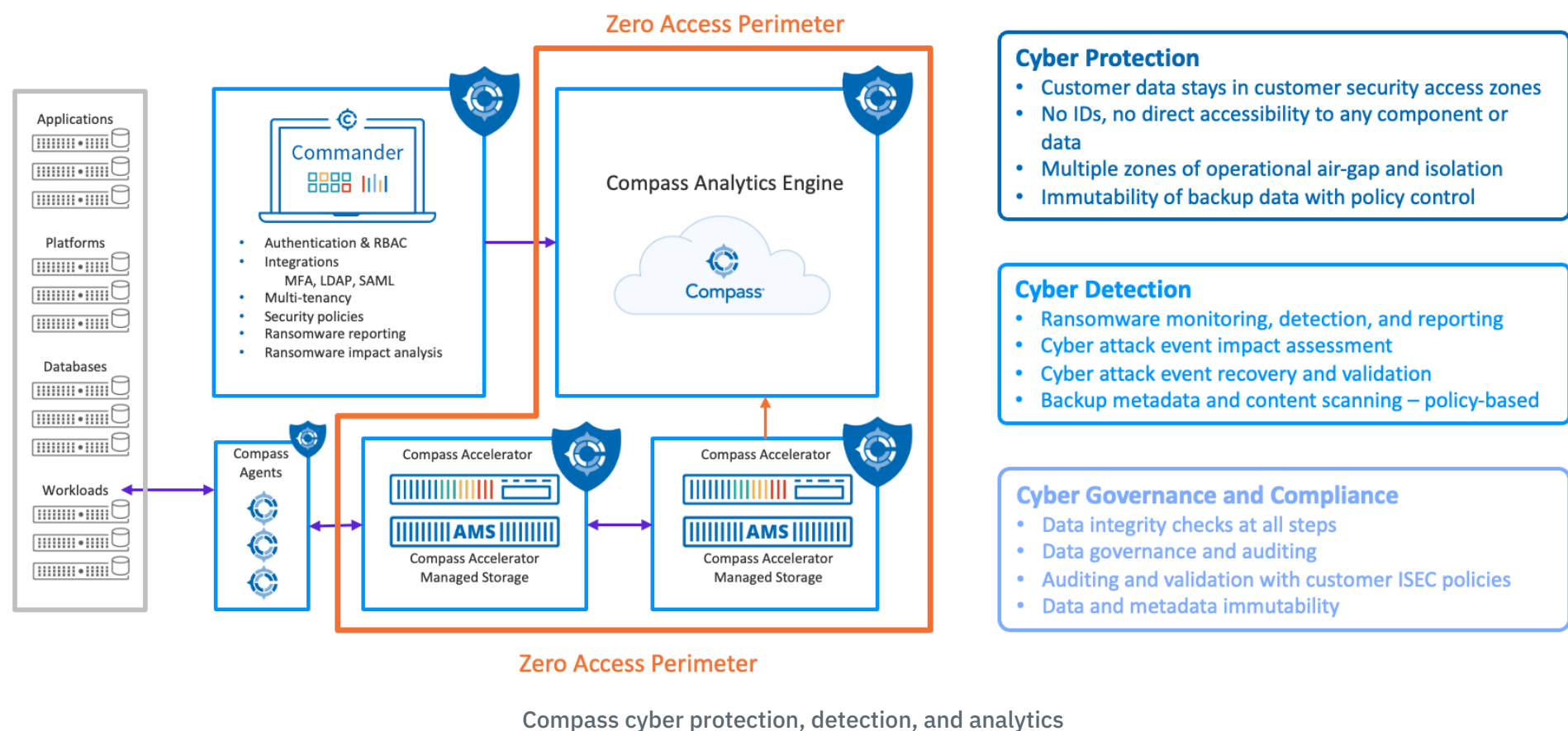
- The customer's PowerVS workspaces, VSIs, and their workloads, are securely connected through corporate cloud networking to the Shared Compass Vaults in IBM Cloud regions or to Dedicated Compass Vault in IBM Cloud or on-premises.
- Second copies of backup data are automatically made to a replication-paired Compass Vault in another cloud region or in another client location (for Dedicated Vault deployments).
- On-premises Power workloads can be backed up to the Compass Dedicated or Shared Cloud Vaults and managed through a consolidated user experience.



Data protection and resilience with Compass

This next figure overviews Compass cyber security protections.

- **Cyber protection** - Compass automation establishes a Zero Access perimeter around the Compass Vaults (that contain backup data) and the Compass Analytics Engine. There is no operational access into these components which eliminates cyber-attack vulnerabilities experienced with other backup products.
- **Cyber detection and impact analysis** – Compass monitors for dozens of data distortion patterns that might indicate a cyber event. Suspicious events initiate cyber event impact analysis that gives insights into possibly infected systems and files and identifies recommended recovery points.
- **Cyber governance and compliance** – Continual data collection and monitoring of the backup environment keep Compass customers in an audit-ready posture for backup and also assist with satisfying compliance requirements.



## Use cases and deployment patterns with Compass

In this section, we will discuss the primary use cases utilizing BaaS with Compass and the deployment patterns in IBM Cloud or client locations. We will cover the best practices when designing the cloud reference architecture and security and compliance considerations. We will end the section with a few real-world client case studies.

## Primary use cases

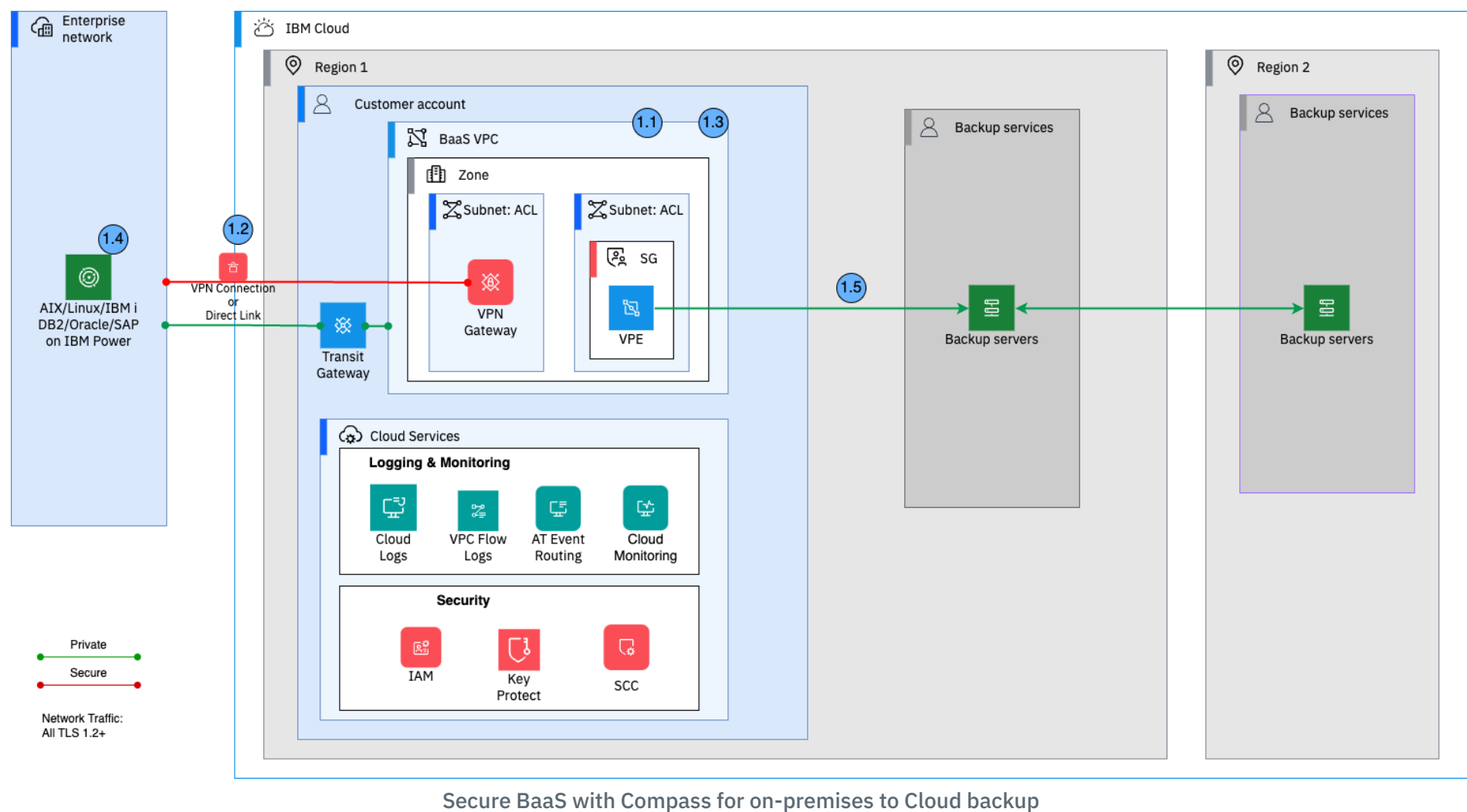
In earlier section, we discussed clients' needs for secure backup to support business continuity and cloud strategy. In this section we will dive deeper into the following use cases:

- Secure backup from on-premises to cloud
- Set up a dev/test environment on PowerVS in cloud
- Secure cloud-to-cloud backup
- Secure backup to a Dedicated Compass Vault at client location

## Secure backup from on-premises to cloud

IBM Power is the foundational platform for mission-critical workloads. Many mission-critical workloads continue to run on-premises due to the control, performance, and security that on-premises infrastructure offers. These workloads often support essential functions—such as ERP, financial transactions, and healthcare systems—that demand low latency, high availability, and strict data compliance. For mission-critical workloads, secure backup is essential to ensure rapid recovery and data protection in the event of system failures, cyberattacks, or natural disasters.

Figure below is the reference architecture for secure backup from on-premises to IBM Cloud.



Secure backup from on-premises to IBM Cloud:

- 1.1 Log in to IBM Cloud and provision Secure Automated Backup with Compass from IBM Cloud catalog.
- 1.2 Set up secure network connection between on-premises to IBM Cloud, via VPN or Direct Link.
- 1.3 Enroll systems and applications to be protected on Compass Commander UI (“SYSTEMS” tab) and enable the backup. For IBM i data protection, you configure a Virtual Tape Library (VTL) on the Compass Vault and then you configure the Compass VTL to your IBM i system as an iSCSI target VTL. You then perform your BRMS or SAV operations to the Compass VTL.
- 1.4 Install compass agent if needed and configure VPN IP addresses to the Compass Vaults.
- 1.5 Backup data is vaulted in multiple, isolated security zones.

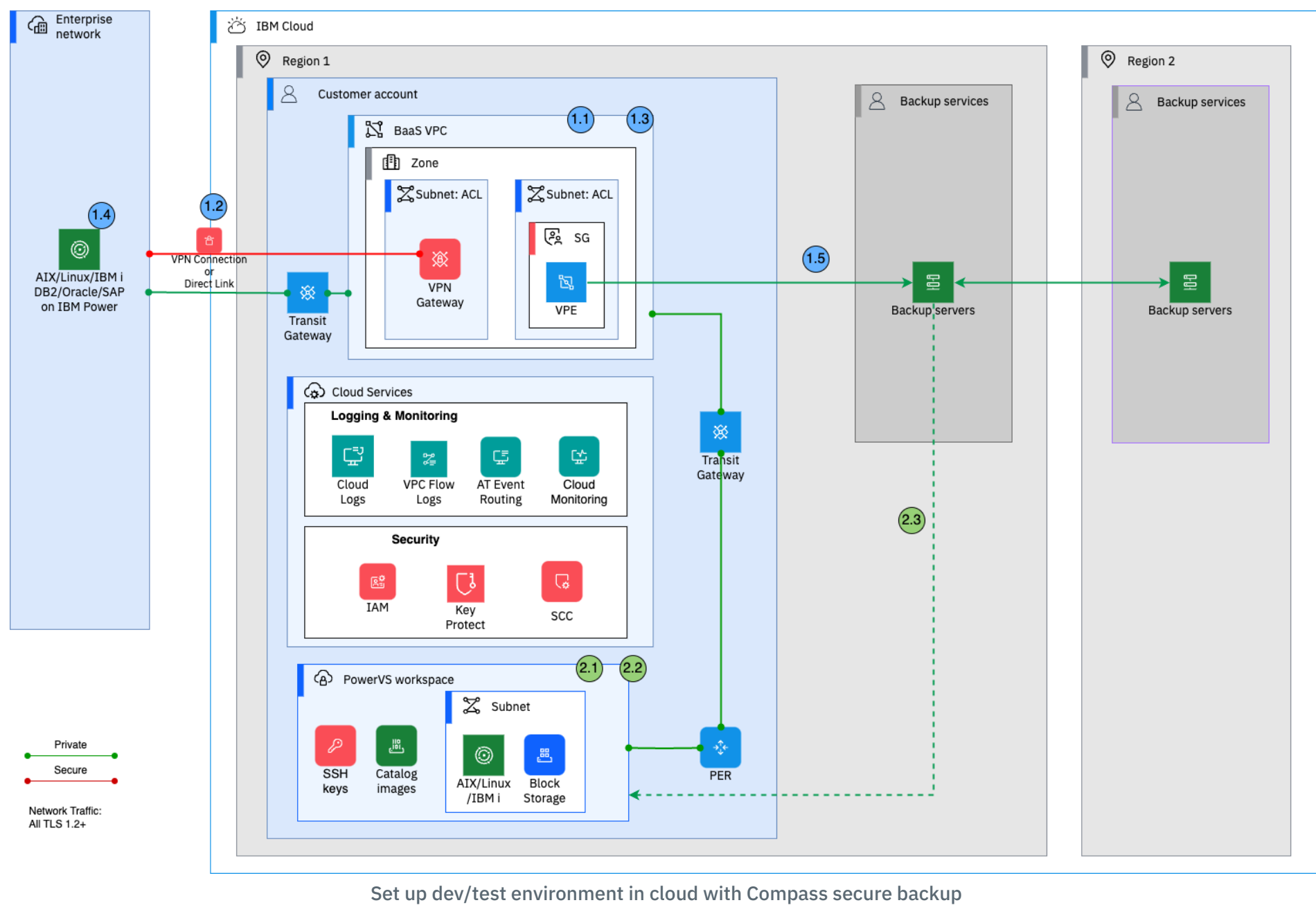
A few things to note:

- BaaS VPC: When the Compass BaaS service is created from the IBM Cloud Catalog, a backup Virtual Private Cloud (VPC) and Virtual Private Endpoints (VPEs) are created automatically by Compass to securely connect corporate cloud networking to the Compass Vaults in IBM Cloud. Refer to [Backup for AIX and Linux instances](#) or the Compass Quick Start Guide for IBM i Data Protection for more details.
- Secure backup service replicates data to a replication-paired Compass Vault in another cloud region. Supported data center pairs can be found in [this cloud doc page](#).
- Enterprise network can be connected to IBM Cloud via Direct Link or VPN.
- IBM Cloud services can be used to manage logging, monitoring, and security of the cloud infrastructure.

## Set up a dev/test environment on PowerVS in cloud

As a foundational step in a cloud strategy, setting up a development and testing (dev/test) environment in the cloud allows organizations to experiment with cloud capabilities in a low-risk, controlled setting. This approach lets teams take advantage of cloud resources—such as rapid provisioning, scalability, and on-demand compute power—without impacting critical production systems. By moving dev/test to the cloud, enterprises can test applications in different configurations, develop new features, and collaborate more effectively while controlling costs and reducing infrastructure dependencies. Starting with dev/test also provides valuable experience for IT teams in managing cloud environments, setting up security protocols, and refining automation and monitoring practices before larger workloads are migrated. This phased approach helps organizations build confidence and expertise, ensuring a smoother and more secure transition as they expand their cloud footprint.

Figure below is the reference architecture for setting up dev/test environment in IBM Cloud using the secure backup established in the previous step.



Once enterprises have the secure backup in cloud, they can create dev/test environment using the backup:

- 2.1 Provision PowerVS environment in IBM Cloud.
- 2.2 Initiate restore from Compass agent UI (or from BRMS or SAV commands for IBM i restores).
- 2.3 Compass server will use the backup data in COS to restore the dev/test environment.

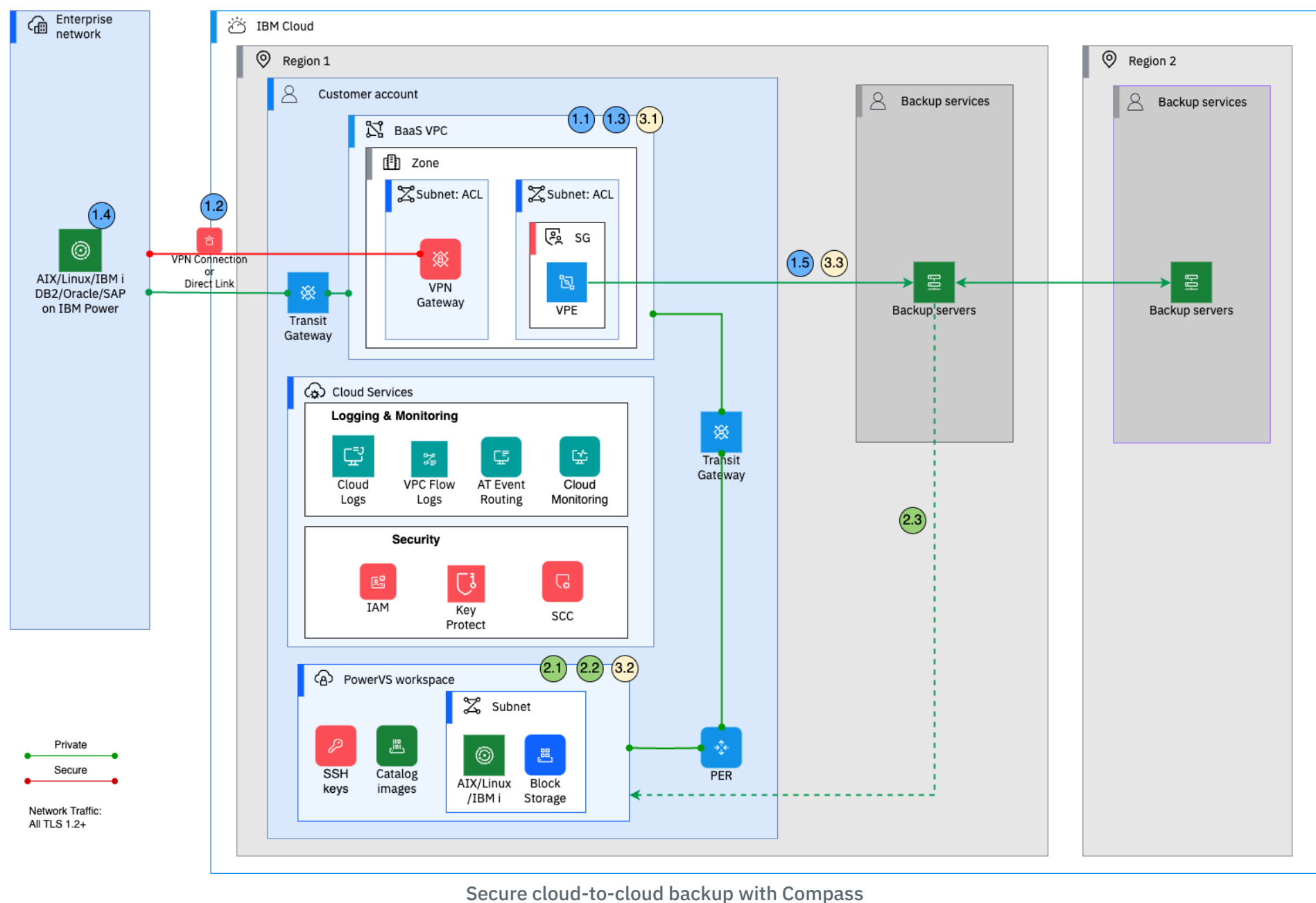
A few things to note:

- The environment to be restored could be in the primary or secondary region. If it is in the primary region, the VPE created for the secure backup instance can be used, otherwise, a VPE may need to be created to connect to the secondary backup server.
- The PowerVS workspace and environment for the restore needs to be created.

## Secure cloud-to-cloud backup

Secure cloud-to-cloud backup is increasingly important as organizations adopt hybrid cloud or multi-cloud strategies, needing to protect data across multiple cloud environments. Unlike traditional backups, cloud-to-cloud backup provides redundancy and resilience by creating secure, encrypted copies of data in a separate region within the same provider or a different cloud provider. This approach protects against cloud service outages, accidental deletions, data corruption, and even ransomware, ensuring that data is recoverable no matter where an issue occurs.

Once the environment is in cloud, figure below is the reference architecture for secure cloud-to-cloud backup.



Here are the steps for secure cloud-to-cloud backup with Compass:

- 3.1 Provision compass service if needed.
- 3.2 Install compass agent (or Compass VTL for IBM i) if needed.
- 3.3 Schedule compass backup (or initiate BRMS or SAV commands for IBM i protection).

A few things to note:

- To back up AIX, Linux, or IBM i workloads in PowerVS workspace in cloud, the BaaS VPC and the Power Virtual Server workspaces are required to be present in the same region and connected by using the local Transit Gateway. Compass automation creates these connections when the Compass service is created from the IBM Cloud Catalog.
- Data are backed up to the Compass backup Vault and then replicated to a paired, secondary Compass Vault in a separate region for added resiliency.
- Multiple LPARs in PowerVS workspace can use the same secure backup servers. For LPARs in the second backup server site, VPE may need to be created.

## Secure backup to a Dedicated Compass Vault at client location

Compass Dedicated Vault options enable clients to maintain their data and workloads on their own sites in locations of their choice. Secure Automated Backup with Compass supports deployment allowing Compass Dedicated Vaults to be deployed in customer's IBM Cloud account or on-premises at client locations.

Here are the steps for deploying Compass in a Dedicated Vault environment:

- Contact your IBM Cloud or partner seller for a customized solution proposal including backup compute and storage for the Compass Vaults in the client's IBM Cloud account or at client locations.
- Provision the Secure Automated Backup with Compass service.
- Install preconfigured Compass Vaults either in the client's IBM Cloud account or at client locations.
- Connect the Compass Dedicated Vaults to your Power workloads.
- Register new systems to Compass Commander and install Compass agents (or configure a Compass VTL in Commander for IBM i protection).

A few things to note:

- The Compass Vaults will be preconfigured with private IP address(es) appropriate for the client locations.

## Best practices from IBM Cloud for Financial Services

[IBM Cloud for Financial Services](#) is designed to build trust and enable a transparent public cloud ecosystem with the features for security, compliance, and resiliency that financial institutions require. IBM Cloud Framework for Financial Services consists of a comprehensive set of control requirements, detailed control-by-control guidance, reference architectures, tools and services to efficiently and effectively monitor compliance, remediate issues, and generate evidence of compliance. This framework was developed in collaboration with leading financial institutions, regulators, and technology partners to provide ongoing governance for the new and changing regulations, as well as bank and public cloud requirements.

When designing the cloud infrastructure, one can refer to the [best practices](#) recommended by IBM Cloud Framework for Financial Services. Here are a few highlights:

- The design should enable a zero-trust model, ensure separation of duties and restrict the access privileges of authorized personnel.
- Maintain non-production environment separately and follow best practices for each environment.
- Enforce information flow policy and protect the boundaries of the applications.
- Use bastion host for operator actions.
- Implement operational logging and monitoring, and keep audit events.
- Encrypt data at rest and in transit.
- HA and DR support.
- Implement regular scan and use endpoint detection and remediation (EDR) tools

## Security and compliance from Compass

Compass auditing provides a comprehensive package of validation and security features such as audit logging, security auditing, security testing, and Vault health monitoring.

Compass also provides a comprehensive Audit Framework that enables customers to govern their backup environment and operations according to their internal processes and requirements. The Compass Audit Framework executes daily processes to examine all facets of every Compass Vault worldwide. Results are posted and analyzed by the Compass Analytics Engine. Any exceptions identified by the Compass analytics automatically trigger a two-phase notification and review process. Audit results are also available for integration with customer IT security policies and systems through the Compass Audit API. The Compass Audit Framework is extensible for customer specific audit and compliance requirements.

The Compass solution also includes tight integration with ServiceNow, Remedy, and other system management tools so you can rest assured that every event or alert is tied directly to corporate consoles and systems.

Compass implements comprehensive stewardship and governance over:

- All backup data,
- Compass infrastructure,
- operational activities,
- data locality requirements,
- administrative and user access,
- policy changes,
- and all aspects of the Compass solution and operations.

In addition, Cobalt Iron itself complies with stringent laws, policies, and procedures, and is SOC2 certification compliant, proving by third party validation and penetration testing the high levels of information security practiced.

Compass also meets the stringent Sheltered Harbor Vaulting requirements for financial organizations and has a Sheltered Harbor endorsed option.

## Compass client case studies

### Client case study 1: IBM CIO office

The IBM Chief Information Officer (CIO) organization leads IBM's internal IT strategy and is responsible for delivering, securing, modernizing and supporting the IT solutions that IBM employees, clients and partners use to do their jobs every day. According to IBM's IT security standards for backups, applications must have data backup solutions based upon their business criticality value.

The CIO organization implemented a cloud-based data protection solution using [Cobalt Iron](#) and IBM technology, including [IBM Storage Protect](#) and [IBM Storage FlashSystem](#). Cobalt Iron offered a centralized self-service portal to control and configure backups, schedules and policies. It also provided a dashboard to see the status and health of the protected environment. Storage Protect provided data resilience for physical file servers, virtual environments and Software as a Service (SaaS) applications while IBM FlashSystem delivered flash array storage with low latency.

With this new enterprise backup solution, the CIO organization delivered a unified user experience by having a single-entry point for all application owners to configure and maintain the IBM backup infrastructure. About 400 application owners can now leverage a single portal to configure, schedule, create and restore backups. The Cobalt Iron portal simplifies the backup and restore processes for applications owners to protect petabytes of critical production

application data.

Refer to [this link](#) for more details.

## Client case study 2: Global banking giant

This global bank has a very complex environment with over 1,500 branches, dozens of data centers worldwide, and hundreds of PBs of data to be protected. Their previous backup operations were outdated, complex, consisting of hundreds of backup servers, dozens of tape library models, many vendors and service providers, and resulting high risks and costs.

After an extensive vendor evaluation and bakeoff, this company chose Compass to replace all of their worldwide backup products and complex operations. The Compass platform outpaced the competition in several key areas including industry-leading cyber security, automation of operations and updates, migration of data off legacy products, and the overall solution value.

The transformation of this customer's large and complex legacy backup landscape into a modern, tapeless, hybrid, SaaS delivery solution is delivering significant financial and cybersecurity benefits.

## Client case study 3: Global apparel and footwear company

This worldwide retail giant faced a myriad of challenges with their aging backup configuration which was a complex mix of many backup products including ArcServe, TSM, Avamar, Data Domain, and others. The collection of backup products presented security challenges, visibility and governance issues, and concerns regarding timely recovery. Multiple Managed Service Providers added an additional layer of complexity and unknowns to this corporation. Consistently protecting their cloud workloads was another challenge.

Their new CISO demanded a more secure, more automated solution that could deliver higher security, higher performance, reliability, and simplification of backup processes.

This corporation chose Cobalt Iron Compass over all the competition based on their key requirements for foundational security for backup operations and data, simplified operations and maintenance, unified reporting, cloud and on-premises support, and overall solution value. Compass is delivering on all key data protection goals for this company and is being extended as their single data protection platform for all international and hybrid environments. In addition, this company has extended its Compass use and is now leveraging the Compass Tape Gateway VTL to protect their IBM i applications and systems.

## Execution and backup in action with Compass

---

### Pre-implementation planning

Customers and IBMers can request a Compass sizing by filling out the [sizing questionnaire](#). This will provide an estimate on Compass solution sizing and costs for the customer.

The Secure Automated Backup with Compass service in the IBM Cloud includes preconfigured Shared Compass Vaults in various IBM Cloud data centers that are ready to service PowerVS and on-premises Power workloads. For Compass Dedicated Vault deployments, Compass Vaults are preconfigured and shipped for installation in the IBM Cloud or at client locations.

When the Secure Automated Backup with Compass solution is created from the IBM Cloud, automated provisioning of the required cloud resources (cloud networking, transit gateway, VPC for Compass, VPEs, etc.) is performed by Compass. For Dedicated Vault deployments, proper connectivity to the IBM Transit Gateway is required for the Power workloads as well as the Compass Dedicated Vaults at client locations.

Provisioning of the customer into Compass is also automatically performed including new Compass organizations for the customer, customer user account, default retention policies for different PowerVS workloads, and backup schedules.

Costs for Compass are determined based on amount of backup data stored after incremental forever, deduplication, and compression.

For more complicated environments including Compass Dedicated Vaults, customer workloads on-premises, or in other clouds in addition to IBM PowerVS, please contact [contact Cobalt Iron](#) for assistance.

### PowerVS environment setup

IBM Cloud deployable architecture is cloud automation for deploying a common architectural pattern that combines one or more cloud resources. It offers a modular, flexible foundation for businesses to build, deploy, and manage applications securely in the cloud.

IBM Cloud offers a few different flavors of deployable architectures that provide an automated deployment method to create an isolated Power Virtual Server workspace and connect it with IBM Cloud services and public internet. For example, you can create a simple [quick start environment](#) for quick testing, [extend current environment](#), or set up [SAP HANA environment](#). For more information on the various Power Virtual Server deployable architectures, refer to [Power Systems Virtual Server with VPC landing zone](#) documentation page.

Once you decide on the deployable architecture to use, you can deploy the environment using a project in IBM Cloud.

- To deploy the Power Virtual Server environment of your choice, follow the detailed instructions on [Deploy using Projects](#).
- Follow the [Client to site VPN](#) if you need to set up VPN for operators.

## Compass backup operations

Refer to Compass documentation for optimal, current usage guidance.

- [Getting Started with Compass](#)
- [Secure Automated Backup with Compass](#)
- [Installing Agent Software Support](#)
- [Oracle on PowerVS](#)
- [DB2 on PowerVS](#)
- [SAP HANA on PowerVS](#)
- [Compass Quick Start Guide for IBM i Data Protection](#)
- [Compass Tape Gateway VTL User's Guide](#)

TODO: Check first and last link here. Links for the last two items.

## Unified backup across platforms

Cobalt Iron Compass supports all of the systems and applications that IBM Storage Protect does plus many additional ones. Compass allows consistent management of diverse workloads across on-premises and various cloud platforms through a consolidated management experience. Compass platform support includes:

- Systems: AIX (back to 7.1), HP-UX, Linux on Power (SLES and RHEL), Linux on Power Little Endian (SLES, RHEL, Ubuntu), Linux x86\_64 (SLES, RHEL, Ubuntu), Linux on Z, MacOS, Solaris, Windows (back to 2012), and IBM i (v7r2 and later)
- Databases: SQL, Oracle, Db2, Informix, MongoDB, MySQL, MariaDB, Sybase, and others
- SAP, SAP HANA
- Email: Exchange, HCL Domino
- IBM Storage Scale/GPFS
- Virtualization platforms: VMware, Hyper-V
- NAS: NetApp, Isilon, Windows File Servers, most NAS devices
- Containers: OpenShift, Kubernetes (via technology plug-in)
- Cloud applications: MS365 (via technology plug-in), AWS services, Azure SQL and other Azure services, Google services, etc.

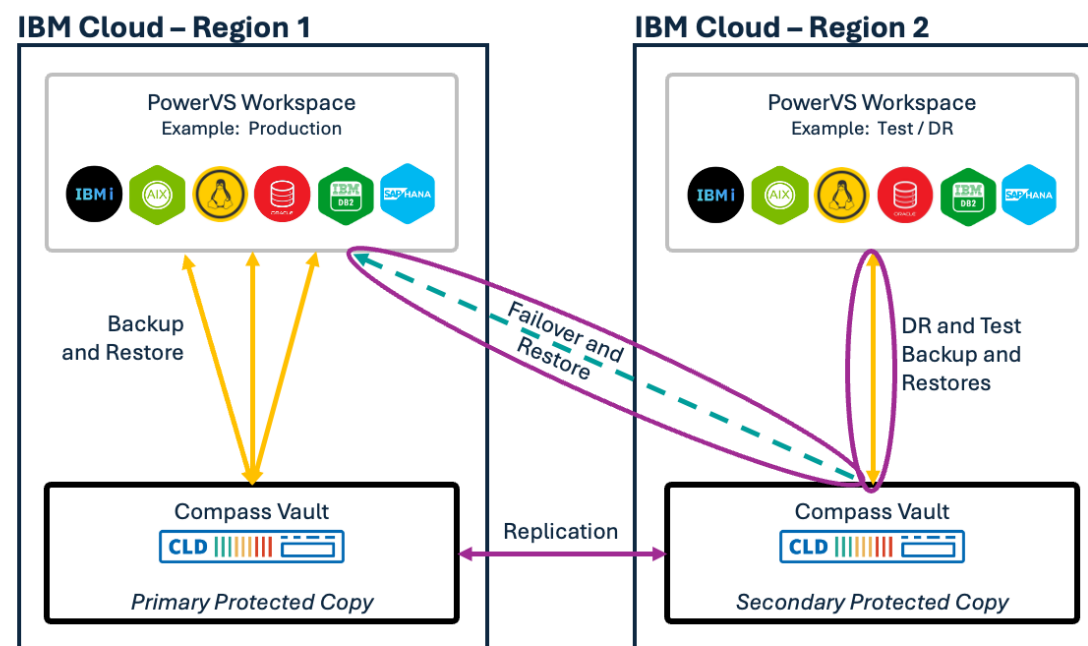
## Strategic summary and expanding beyond backup

---

### Cloud strategy alignment

Secure backup is essential not only for business continuity but also for supporting an effective cloud strategy. By creating secure, encrypted backups, businesses can safely migrate workloads, test cloud environments, and ensure data redundancy across hybrid and multi-cloud setups. Secure backups provide a reliable foundation for scaling operations to the cloud, as they allow data to be restored or replicated in different cloud regions or providers, ensuring resilience and flexibility. This approach not only safeguards against data loss but also facilitates cloud adoption, enabling seamless data mobility, regulatory compliance, and risk management as companies expand their cloud infrastructure.

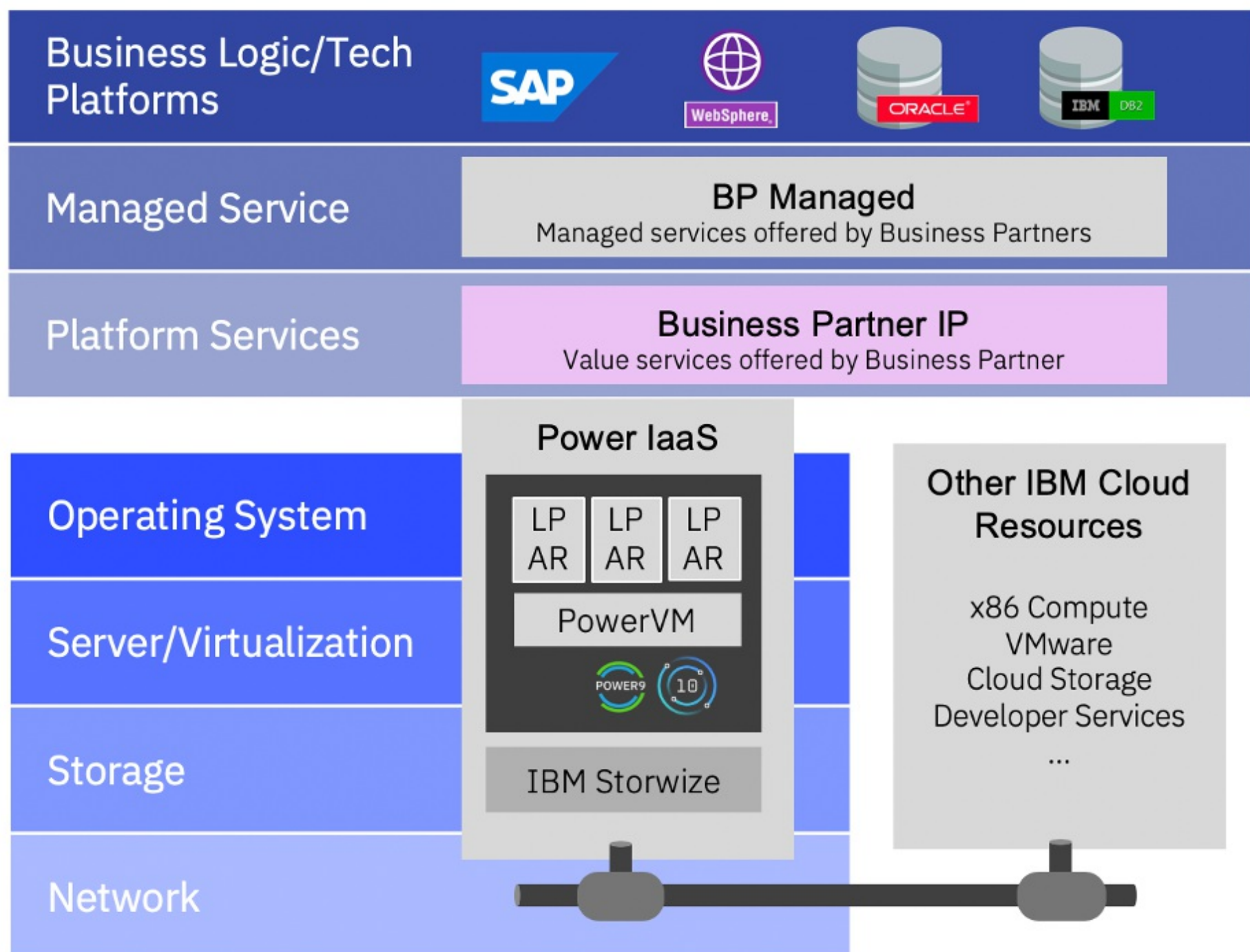
As highlighted in the following figure, the backup images can be used to restore an environment in cloud. As discussed in section 3.1.2, as enterprises start to embrace cloud strategy, they can rapidly provision a dev/test environment in cloud when needed to take advantage of cloud without impacting critical production systems. This would also bring cost advantages to provision the environment with the right sizing only when needed.



Restore secure backup to a working environment

## Integration with IBM Cloud Services

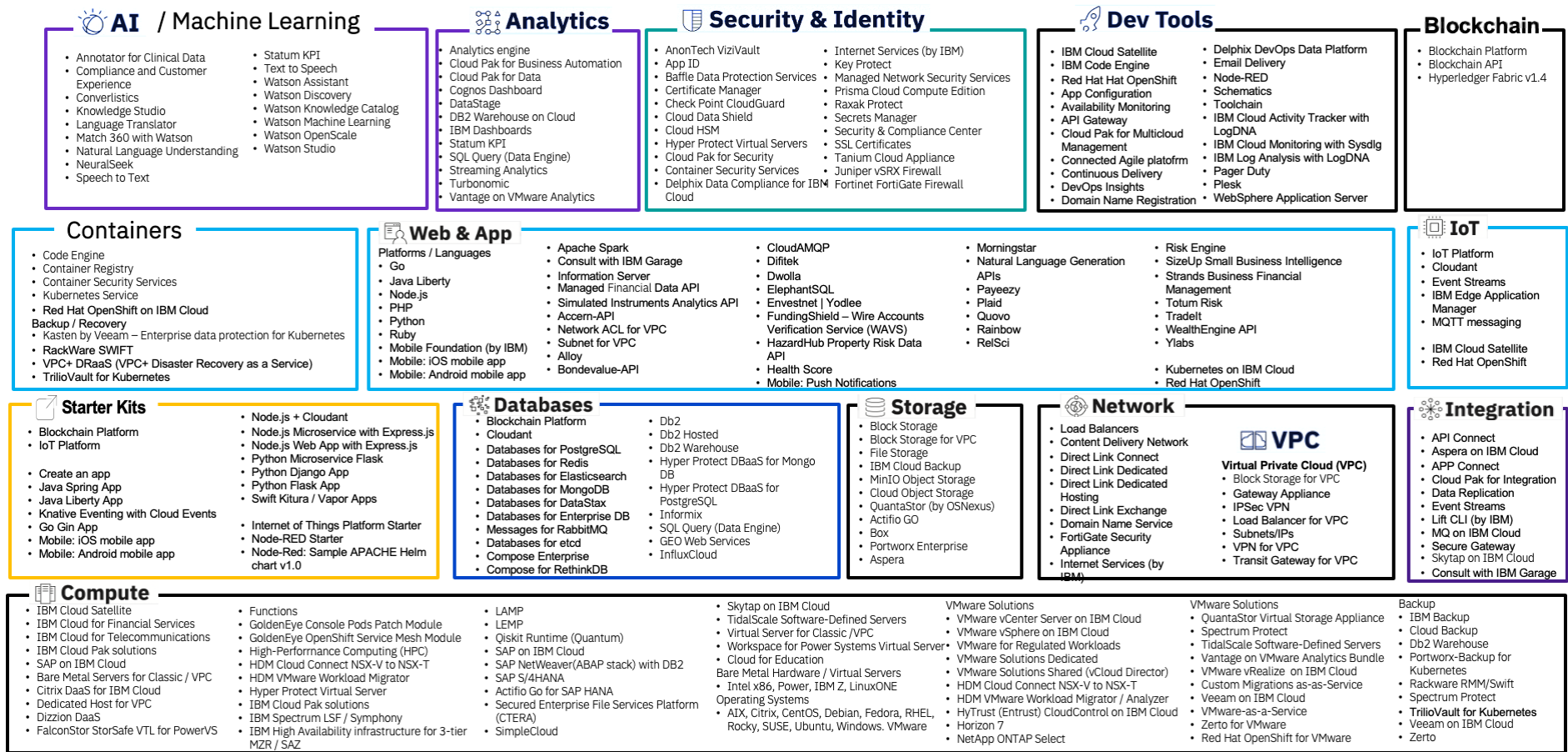
IBM Power Virtual Server is an IaaS offering, and IBM manages the layers up to the operating system level. Clients can integrate with rich set of services provided by IBM and business partners.



Power IaaS

Clients can build applications within IBM Cloud's rich ecosystem, which offers an extensive array of tools, services, and integrations to accelerate

development, enhance functionality, and support scalability. This ecosystem includes a diverse selection of managed services for databases, AI and machine learning, IoT, blockchain, and analytics, allowing clients to create sophisticated, data-driven applications. With built-in DevOps tools and seamless integrations with open-source technologies and third-party platforms, IBM Cloud enables rapid application development and deployment. Additionally, robust security and compliance features are embedded across the ecosystem, allowing clients to meet industry standards while focusing on innovation. This rich environment empowers clients to build adaptable, future-ready applications that can evolve with their business needs.



Sample IBM Cloud services

## Enterprise security and compliance

IBM Cloud offers a robust suite of security and compliance features designed to protect data, manage risk, and ensure regulatory adherence across diverse industries.

IBM Cloud for Financial Services is a secure, industry-specific cloud platform designed to help financial institutions adopt cloud technologies while meeting stringent regulatory and compliance requirements.

IBM Cloud provides multiple security services including unique Key Management Services (KMS) like Key Protect (KP) and Hyper Protect Crypto Services (HPCS) along with confidential computing features (like Hyper Protect Family of services (incl Virtual Servers and container runtime protection) (HPVS)) to protect the data in all these three segments with ownership solely retained by enterprise application owners. With IBM Cloud’s unique feature like Keep-Your-Own-Key (KYOK) even IBM Cloud administrators cannot access the enterprise data.

IBM Cloud Security and Compliance Center provides visibility into your workloads with features such as security and compliance automation, monitoring and assessing compliance across hybrid cloud environments, gathering evidence for compliance needs, increased visibility for your entire organization, and regular reviews for compliance audits.

IBM Power Virtual Server has [compliance certifications](#) that help you establish and strengthen compliance for a wide range of internationally recognized standards, including SOC, ISO 27017, PCI-DSS, HIPAA, and Financial Services Validated.

Cobalt Iron Compass also provides tremendous security features as partially described in sections 2.2 and 3.3 above.

## Summary

IBM Cloud Partner Cobalt Iron provides an automated backup offering for AIX, Linux, and IBM i instances on IBM Power Virtual Server or on-premises, accessible from IBM Cloud catalog. Secure backup is crucial for enterprises in the digital era. Capabilities and security features from Cobalt Iron Compass protect enterprise against evolving threats while enabling business continuity and maintaining data integrity and compliance.

# About the authors

**Yichong Yu**

STSM, IBM Cloud for Financial Services  
<https://www.linkedin.com/in/yichongyu/>

**Greg Tevis**

Vice President, Strategy, Cobalt Iron  
<https://www.linkedin.com/in/greg-tevis-10a5042/>

© Copyright IBM Corporation 2026

IBM Corporation  
New Orchard Road  
Armonk, NY 10504

Produced in the United States of America  
2026-05-04

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at <https://www.ibm.com/legal/copytrade>.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

