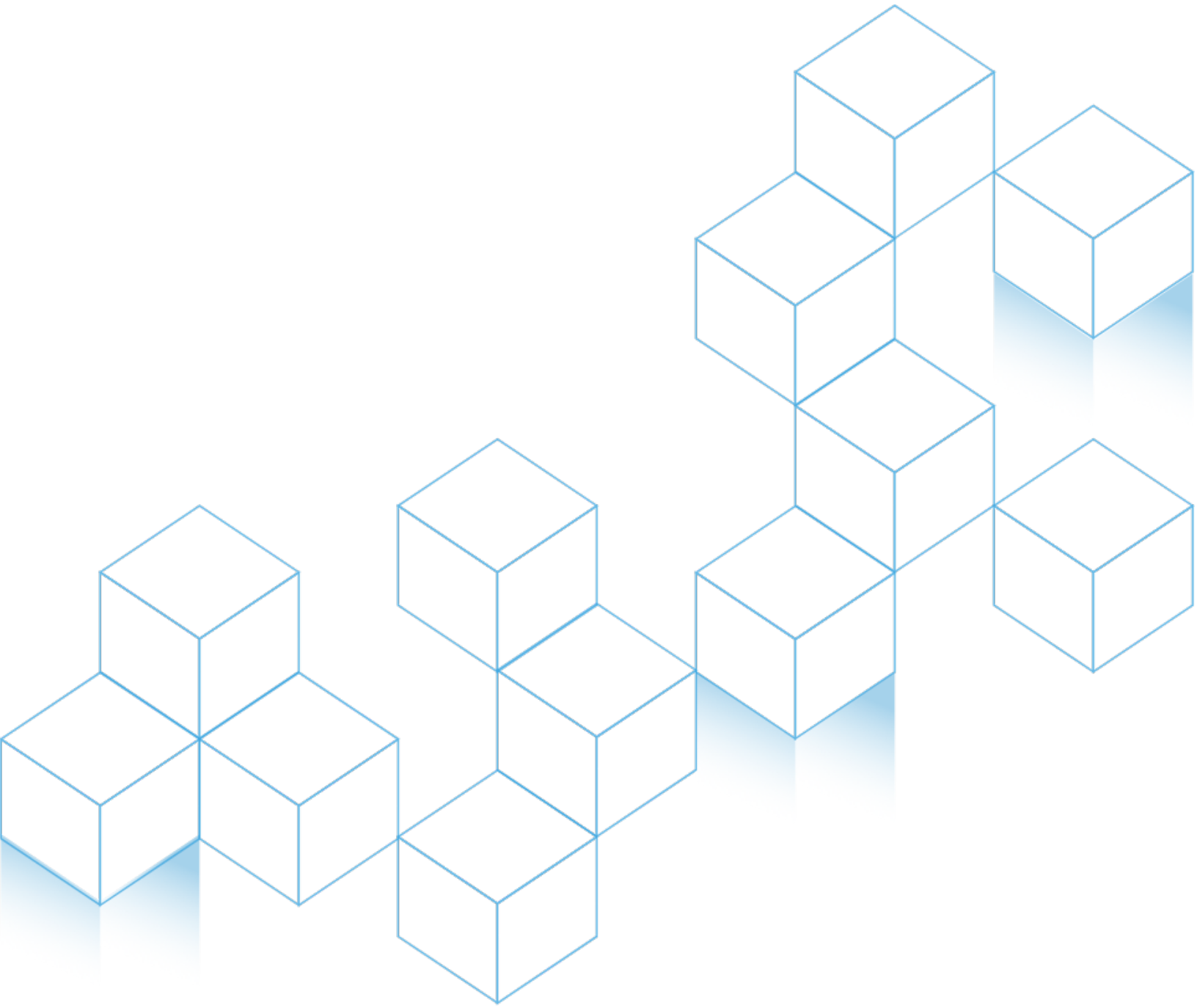
Skytap on Azure

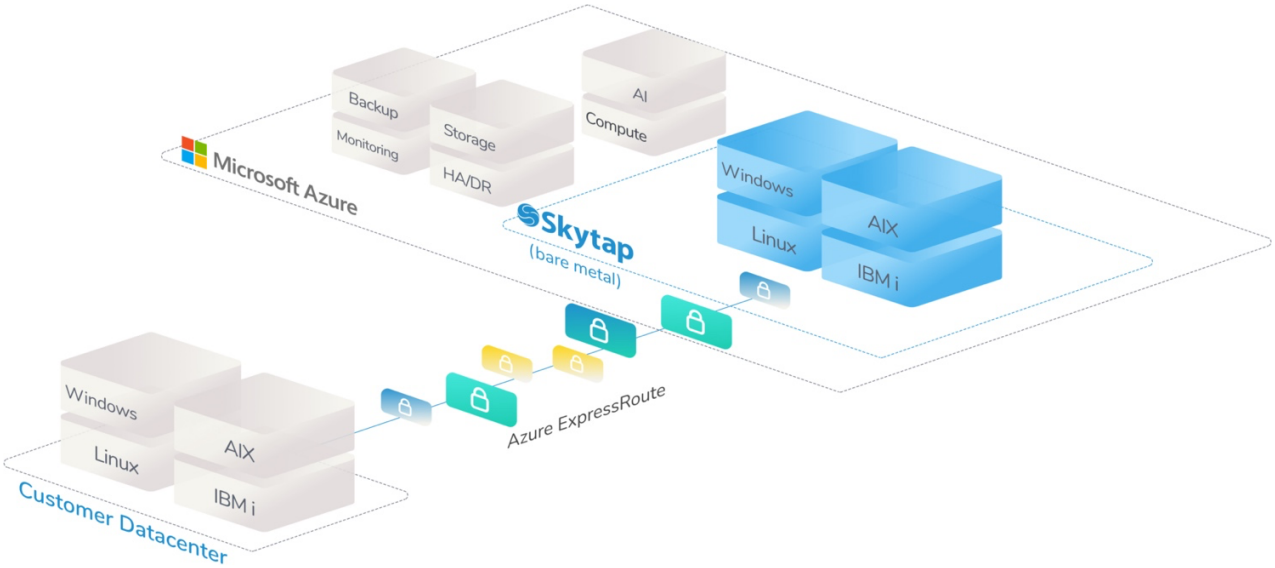
Security and Compliance

2023



Introduction

Skytap on Azure is a cloud service for creating, managing, and sharing virtual machine environments. With Skytap, your traditional IBM Power and x86 workloads can run natively in the cloud in Microsoft Azure on the latest IBM Power hardware, procured and maintained by Microsoft.



Entrusting your business-critical applications to a public cloud service provider depends on an awareness of available security controls and an understanding of the shared responsibility operational model. Skytap, together with Microsoft, is committed to providing this transparency to support your data security, privacy, and compliance objectives in Skytap on Azure.

The purpose of this white paper is to offer those evaluating Skytap on Azure an overview of the security controls, accreditation, and task obligations across parties—Skytap, Microsoft, and the customer. The information presented here is meant to help customers understand the security measures in place as a crucial step in developing a comprehensive security strategy for the cloud.

This paper is not a detailed specification of Skytap on Azure security functionality nor a replacement for Skytap or Microsoft support documentation.

Contact your Skytap representative or refer to the Microsoft Trust Center for further information beyond this document.

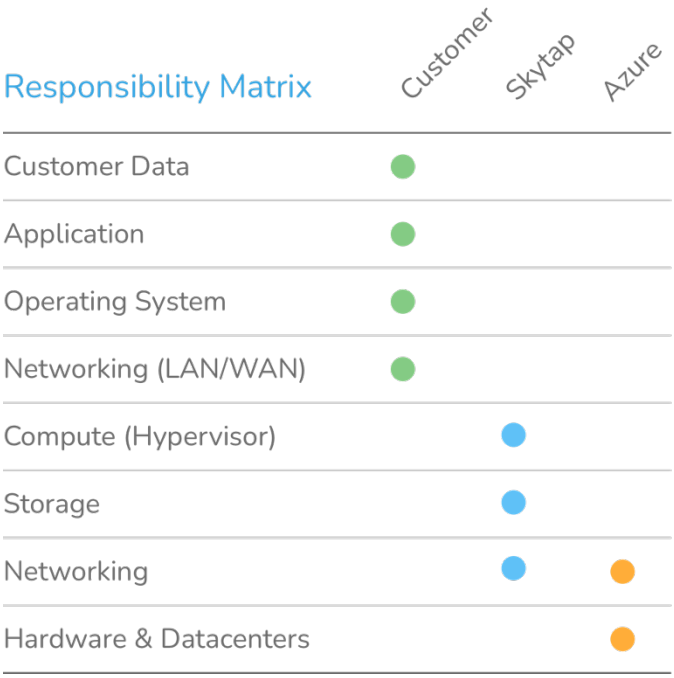
Skytap Commitment to Security and Compliance

Skytap designs, builds, and operates its cloud platform services following known data security best practices. Every component used to build the Skytap platform has been selected or built with security in mind.

Additionally, Skytap on Azure offers a range of default and optional security features that can be implemented at the account, user, and environment level. Account administrators have access to comprehensive documentation on these built-in controls and generalized best practices on their use within individual Skytap environments.

Skytap performs regular assessments across technology, people, and operational processes based on common risk management frameworks. Skytap uses outside auditors to validate these efforts independently.

As is typical with cloud platforms, the responsibility for safeguarding your data, users, and applications running on Skytap on Azure is shared between the customer and the provider. In the case of Skytap on Azure, the division of responsibilities falls across multiple parties:



As illustrated above, Skytap and Microsoft are accountable for the platform. Customers are responsible for the way they use that platform.

For its part, Skytap continuously reviews and improves Skytap on Azure security capabilities to ensure the platform meets the requirements to mitigate risks today and in the future.

How this paper is organized

The Skytap on Azure security and compliance practices described in this white paper are presented using the familiar topic areas of the Microsoft Azure Trust Center:

Security	Skytap on Azure's multi-layered security foundation
Privacy	Protecting the confidentiality of data stored and processed in Skytap on Azure
Data Protection and Privacy Regulation	Addressing Data Subject Requests (DSRs) in Skytap on Azure
Data location	Data residency options and regional data storage for Skytap on Azure
Compliance	Achieving compliance with Skytap on Azure

Each section includes a brief overview and references to more detailed information from either Microsoft or Skytap, as appropriate, based on the division of responsibility.

Security

Skytap on Azure employs a robust set of controls and operational best practices to provide a multi-layered security foundation to natively run AIX, IBM i, and Linux on Power workloads in the Microsoft Azure cloud. These security capabilities—spanning Skytap and Azure service components—build upon the controls and features of the layers below. When combined, they provide fundamental safeguards against cyber-threats and help ensure the cloud platform's availability and integrity.

Skytap on Azure customers use these features to establish a secure environment to migrate, run, and protect their applications in the cloud.

Datacenter infrastructure and physical security

Skytap on Azure operates on IBM Power9 server hardware located within the Microsoft Azure datacenter and directly integrated with the Azure network. Microsoft is solely responsible for the procurement, maintenance, and security of these hardware assets.

Skytap employees do not have direct physical access, at any point, to the systems and infrastructure used to deliver Skytap on Azure services.

Microsoft's datacenter infrastructure security remit includes:

- Designing, building, and operating all the physical facilities in which Skytap on Azure is available.
- Controlling and monitoring access to the facility's perimeter, building entrance, and the datacenter floor using state-of-the-art physical security. Access is restricted to only Microsoft employees with approved business justification.
- Staffing and training all datacenter security and operational personnel.
- Installing, maintaining, and decommissioning all equipment at the end of service according to Microsoft's rigorous data handling and hardware disposal procedures.
- Conducting regular physical security reviews and meeting with compliance standards, such as ISO 27001, SOC 1, and SOC 2.

Skytap security personnel regularly review the Microsoft Azure SOC 2 audit report to ensure all the controls mentioned above operate effectively. More detail is available in the latest Skytap SOC 2 report, available upon request from your Skytap representative.

Network security

Skytap on Azure leverages network components and connectivity at numerous platform layers:

- Edge networking, including private network connections like Azure ExpressRoute.
- Virtual network switches within the hypervisor hosting each Skytap environment.
- Inter-configuration network routing (ICNR) between Skytap environments.
- Skytap service fabric (management network) isolates underlying platform and data channels from customer resources.

Skytap and Microsoft implement numerous network access controls and resiliency mechanisms to safeguard data privacy and ensure that all customer network traffic flows on fully isolated virtual networks.

The Azure datacenter network utilizes a wide range of physical and virtual network layer controls to mitigate against unauthorized traffic flows, denial of service attacks, and maintain logical tenant segmentation. Skytap builds upon this foundation.

Within Skytap on Azure, virtual machines are connected to one or more separate virtual networks. Each network is assigned a unique Virtual Local Area Network (VLAN) as defined in IEEE 802.1Q. Every network packet sent by a virtual machine is tagged with a VLAN identifier, and intermediate physical and virtual switches ensure the packets reach only virtual machines (VM) on the same private subnet. This VLAN mechanism extends to the virtual switches within hypervisors hosting Skytap VMs.

The assignment of VLAN tags and switch provisioning is managed within the Skytap service fabric and is invisible to virtual machines and users. This approach prevents VMs from discovering or forging VLAN assignments. It also mitigates the risk of leaked or sniffed network traffic between Skytap on Azure customer private networks. Customers can enable traffic routing between environment networks within their Skytap account if desired, but it is disabled by default.

Internet traffic is controlled by two levels of firewall devices: one at the Skytap on Azure network perimeter and another at the customer's Skytap environment network perimeter. Customers can also deploy virtual network appliances within their virtual networks, configure firewall policies within their virtual machines, and manage their virtual network services, including DNS or DHCP.

Skytap on Azure customers can leverage these mechanisms to manage access to their virtual machines and networks, from other Skytap environments, with other Azure Services, and from the Internet:

- **Internal Network Access Controls** - Each virtual network is isolated from all other virtual networks within Skytap. Users can enable automatic routing between networks within a single environment, or between networks within different environments in the customer's own account. Networks within different customer accounts cannot be connected.
- **Outbound Internet Access Controls** - Virtual machines access the Internet through a default gateway provided on each network. Internal private addresses are mapped to a public Skytap address using IP masquerading (NAT). Skytap users have the ability to disable outbound access at any time.
- **Inbound Internet Access Controls (Port Forwarding)** - Networks within Skytap are generally not visible or accessible from the Internet, but customers can selectively allow inbound Internet access for specific network services (e.g., HTTP). Network rules in Skytap permit incoming packets from the Internet on specific ports to reach a specific virtual machine; all other ports remain blocked.
- **Inbound Internet Access Control (Public IP Addressing)** - Customers can also acquire a Public IP address from Skytap and attach the address to individual virtual machines. This allows customers to open all ports for both inbound and outbound Internet access without port mapping.
- **Internal Firewall with Port Forwarding or Public IP Addressing** - Customers can customize their network security posture by deploying and configuring their own virtual network appliances with port forwarding or attached Public IP addresses. For example, a customer can provision a virtual firewall appliance with complex port forwarding and ACL rules on traffic destined to and from other virtual machines within the network.
- **Virtual Private Network (VPN) and Private Networks Connections (PNC)** - Customers can connect to external networks through an IPsec-based VPN and Private Networks Connections with ExpressRoute to securely transfer traffic between an external network (like a network in an on-premises data center or another cloud service provider) and one or more Skytap virtual environments in a Skytap region.

Storage and data security

Access to Skytap on Azure customer data by either Skytap or Microsoft operations and support personnel is denied by default.

Skytap implements a multi-layered approach to protect data while it is at rest and in-flight:

- **Encryption at rest** is implemented for the underlying storage system through the use of Self-Encrypting Disks (SED) with support for AES-256 encryption. The encryption keys are provisioned by the disk controller. Encryption keys are stored in a central secrets management system and pushed to controllers when new systems are

provisioned. Keys are discarded from the controllers when systems are decommissioned, or the controller component of a storage system is replaced for maintenance.

- **Encryption in transit** is enabled by the use Transport Layer Security (TLS) 1.2 or later, to secure communications over the Internet. All Skytap operations, including accessing the Skytap web application; accessing Virtual Machine consoles using Skytap Secure Remote Access or SmartRDP; REST API; and uploading (or downloading) files to (or from) Skytap, are encrypted using HTTPS. Import and export of virtual machine images use SFTP (Secure File Transfer Protocol), though FTP transfer is supported as well for those customers who require it.

Skytap maintains customer data—including VM disk images, asset files, and shared drive contents—in virtualized network-attached data stores and exposes it via independent network file-system mounts. This provides isolation between file data for different customers, and between all disk images: when a virtual machine is run, only the disk images for that particular machine are exposed through the mounted file system, and only during the time the VM is running.

Further, the movement of data between the storage layer and the physical servers occurs on an isolated management network (Skytap service fabric) that is not accessible to customer environments.

Finally, customers can use encryption within guest VM file systems to provide additional security.

Skytap maintains scheduled offsite backups of critical configuration metadata of Skytap on Azure environments for service reliability purposes. However, it is the customer's responsibility to follow data protection and high availability best practices for the applications and business data hosted in their Skytap environment.

Hypervisor security

All customer IBM Power-based workloads are executed in virtual machines hosted on the IBM PowerVM hypervisor. The hypervisor provides strong isolation and logical partitioning of the processor, memory, network, and disk state between virtual machines. This prevents one virtual machine from inspecting the state—or even detecting the existence of—other VMs on the same hypervisor.

The only communication channel between virtual machines is through customer-created virtual networks that are private to the Skytap on Azure environment, and through customer-managed private links between their environments. Customers are not permitted access to the

hypervisor or physical server layers within Skytap. Management of virtual machines is only possible through controls exposed by the Skytap portal and REST API.

Skytap actively monitors and maintains the Skytap on Azure hypervisor fleet to ensure each has the latest security patches and is operating within defined parameters.

Customers have full control of the Operating System and application software running in their virtual machines. Customers are responsible for configuring and maintaining Operating Systems and all application software to ensure the security of their virtual machine environments. This includes password management, patch management, antivirus and malware detection/prevention, and running firewalls to secure their virtual machines.

Access security and identity management

Skytap on Azure is provisioned, accessed, and managed through a combination of the Microsoft Azure portal and the Skytap portal using a modern web browser.

In all instances, Azure and Skytap utilize robust authentication and authorization controls to manage identities and role-based access rights.

Skytap on Azure customers provision their services through the Azure Marketplace. Once provisioned, the new Skytap on Azure account will be automatically configured for single sign-on (SSO) using Azure Active Directory (AAD).

In addition to AAD, Skytap supports Security Assertion Markup Language (SAML)-based 2.0 SSO, making it compatible with an on-premises Active Directory, as well as identity provider services like Ping Identity or Okta. Further safeguards are possible by implementing a two-factor authentication solution that integrates with the SSO solution.

User accounts, access permissions, and roles are fully configurable within the Skytap portal. Roles enable Skytap on Azure administrators to consistently apply granular access permissions—restricted through full administrator privileges—to individual users or groups of users.

User access to the Skytap on Azure website can be further secured by setting policies that restrict login to predefined source IP addresses. IP-based access blocks traffic to the Skytap portal and API from all IP addresses outside of a designated range. For example, customers can require users to both successfully authenticate and access from IP addresses in the company network.

Support for browser activation creates an additional security layer by requiring users to verify their accounts before they can sign in from an unregistered browser. When enabled, all users

will be required to complete a one-time validation code through a channel other than the browser, resulting in a secure browser token.

All Skytap on Azure account activities are logged and recorded for both security review and usage accounting purposes. Up to two years of detailed audit data is available through the Skytap portal and via a configurable webhook service for real time streaming to a URL that you choose.

Operational security

In addition to the security mechanisms built into the Skytap on Azure platform, Skytap operational staff use a number of additional defense and detection tactics and techniques to continuously monitor the service.

- Network and application-level penetration testing is regularly conducted by third parties and Skytap. In the event that vulnerability is found, it is promptly remedied and validated.
- Comprehensive infrastructure monitoring detects and alerts traffic anomalies such as port scanning, and excessive connection rates, then flags the suspect VMs. Any incidents are evaluated and remedied in cooperation with the owner of the suspect VMs as appropriate.
- The Skytap Acceptable Use Policy (AUP) strictly prohibits users from running malware, viruses, and spambots; mounting Denial of Service (DOS) attacks; and hacking security mechanisms.
- Infrastructure servers are locked down, to enable only services that are essential for operation.
- Access to infrastructure systems is restricted to a small staff and Skytap employees do not have direct physical access. Industry-standard authentication, access control, logging mechanisms, and periodic audits are employed routinely.
- Skytap follows a documented process for controlling all access and changes to production environments.
- Vendor/industry notices related to security vulnerabilities in the products that comprise the Skytap infrastructure are routinely reviewed, and relevant patches and updates are applied as they become available.
- Skytap employees are trained on documented information security and privacy procedures.
- Access to customer confidential information is restricted to authorized personnel only, according to documented and audited processes.

- Access to customer data is prohibited except where explicitly authorized by customers for resolving support issues, and in accordance with documented and audited policy.
- Skytap maintains scheduled offsite backups of critical metadata. Restoration tests are performed routinely to ensure validity.

Similarly, Microsoft has well documented practices and procedures on how they manage and operate the Azure production network to secure the datacenter locations hosting Skytap on Azure.

Skytap and Microsoft work cooperatively in response to incidents and service health issues that may impact the availability of Skytap on Azure.

Skytap on Azure service status updates are available via https://status.skytap.com/.

Security best practices

Skytap offers generalized best practice guidance to support Skytap on Azure account administrators in safeguarding their Skytap environments. These best practices are reviewed and updated on a regular basis by Skytap subject matter experts as new security capabilities are added to the Skytap on Azure platform.

The best practice guidance is available from the Skytap Help and Documentation website.

Privacy

Ensuring the privacy and confidentiality of data stored and processed in Skytap on Azure is top priority for Skytap and Microsoft.

This is accomplished through the following practices and techniques:

- Skytap and Microsoft recognize that the customer is the owner of any data that is stored and hosted in the Skytap on Azure services.
- Skytap manages the secure disposal of any storage assets in accordance with the Skytap Information Security Policy. This includes securely wiping any storage devices before disposal.
- As referenced in the data security section above, Skytap secures data while at rest and in transit based on industry-standard data protection and encryption mechanisms.
- Microsoft Azure follows clearly documented standards for data privacy, where applicable to Skytap on Azure service delivery.
- Both Skytap and Azure comply with a number of external privacy standards, laws, and regulations. Details and applicability are dependent on specific Skytap on Azure customer requirements.

Customers are ultimately responsible for protection and disposition of the applications and business data they manage and process while hosted within their Skytap environment.

Law enforcement requests for customer data

Skytap complies with all laws and regulations, including valid law enforcement requests for data.

- Skytap acknowledges and recognizes that the customer is the owner of the data stored and processed in Skytap on Azure.
- Skytap will direct the requesting party to seek the data directly from the customer, wherever possible.
- Skytap does not voluntarily provide any government direct or unfettered access to customer data.

Skytap defers to the Microsoft Azure policy for any customer data requests beyond the Skytap on Azure platform.

Data Protection and Privacy Regulation

Skytap always endeavors to remain compliant with the privacy rights and obligations of applicable privacy and data protection regulations such as the European Union General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) for California residents.

More details are available in the Skytap Privacy Policy and Skytap Omnibus Data Processing Addendum (DPA).

Customers are ultimately responsible for responding to any Data Subject Requests (DSR) to business data hosted in their Skytap environment.

Skytap defers to the Microsoft Azure policy for Data Subject Requests under GDPR or CCPA that are beyond Skytap's control over the Skytap on Azure platform.

Data location

Customers have the ability to specify the Microsoft Azure Region where their data will be stored based on Skytap on Azure services availability at the time of service provisioning.

Skytap may transfer platform administrative data required to operate the Skytap on Azure platform to other Regions for data resiliency purposes. However, Skytap does not transfer any customer application or business data hosted in their Skytap environment.

Customers have the ability to copy, move, or access a Skytap on Azure environments or templates between regions.

Skytap defers to the Microsoft Azure data residency policy for service functionality that is beyond Skytap's control over the Skytap on Azure platform.

Compliance

Skytap is dedicated to providing Skytap on Azure customers with secure cloud infrastructure services, this is reflected throughout our development and production operations practices. The responsibility of maintaining overall security and compliance in the cloud is shared between Skytap, Microsoft, and the customer.

Skytap designs, builds, and operates its cloud platform services following known data security best practices. This includes ensuring the Skytap on Azure platform security controls and operational processes comply with standards, including the Payment Card Industry Data Security Standard (PCI DSS) and ISO/IEC 27001:2013.

Additionally, Skytap maintains EU-US Privacy Shield certification because, regardless of its validity under current EU law, doing so still demonstrates valuable data privacy and security protections when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce.

Skytap also conducts annual SOC 2 Type 2 compliance audits performed by an independent third-party audit firm. The design and operating effectiveness of Skytap controls are evaluated against AICPA Trust Services Criteria for security, availability, and confidentiality. Skytap's SOC 2 audit reports are available to customers upon request.

Skytap defers to the Microsoft Azure compliance documentation for service functionality that is beyond Skytap's control over the Skytap on Azure platform.

Additional resources

Skytap security best practices	https://help.skytap.com/Security_Best_Practices.html
Skytap security improvements: deprecation and end of life (EOL) notices	https://help.skytap.com/kb-eol-notices.html
Skytap Help and Documentation	https://help.skytap.com/
Skytap Blog	https://www.skytap.com/blog/
Microsoft Azure Trust Center	https://www.microsoft.com/en-us/trust-center/product-overview