Top security questions answered for APEX Cloud Services with VMware Cloud

On-premises infrastructure as-a-service that combines the ease of operations of public cloud with control, security, and performance of private cloud.

Q | How can I protect my data and eliminate the complexity of managing my own Enterprise Key Management System (EKMS)?

A: This cloud service comes with built-in cyber resiliency and encryption of data at rest and in-flight, with the key management included. So, customers have security at every level and can be assured that their data is protected from malicious attacks combined with the additional benefit of not having the complexity and burden of managing and owning an Enterprise Key Management System (EKMS). Communication of sensitive information such as authentications, administrative access, and customer information is encrypted with standard encryption mechanisms such as SSH, TLS, and Secure RDP. Data is encrypted with a key that is unique to each SDDC and stored in the Trusted Platform Module (TPM).

Q | Does APEX Cloud Services meet data localization, regulatory, and audit requirements?

A: On-premises as-a-Service solutions address many of the challenges you may face with public cloud, such as security, compliance, and availability concerns. APEX Cloud Services with VMware Cloud helps you meet data localization and regulatory requirements, while also protecting you from malicious attacks with built-in cyber resiliency. Additionally, APEX Cloud Services with VMware Cloud is built on infrastructure that delivers 99.9999% availability[1], enabling you to deliver more value to your organization while maintaining complete control over your data.

Q | Who's in control of my data?

A: You're in control of your data. As a customer, you retain control and ownership of your content and can secure your data as required. Dell Technologies controls the access rights based on the principle of least privilege, which means only the minimum level of access required is granted. Access is provided according to the individual job functions and requirements.

Q | How can I trust that my data is secure?

A: Dell Technologies subscribes to vendor security and bug-tracking notification services. Remediation efforts are prioritized and applied against critical and high-risk issues. Critical patches are installed on time and non-critical patches are included in the pre-defined patch schedule and applied within reasonable timeframes.

Q | How does Dell Technologies connect to my infrastructure?

A: Dell Technologies uses dedicated secure networks to access the management software used to operate the infrastructure. For APEX Cloud Services with VMware Cloud, Dell Technologies uses an encrypted VeloCloud SD-WAN connection to extend the management network to the customer location. Only authorized personnel involved in the operation and maintenance the service can access this management network.

## Q | What happens after my subscription is over?

A: Dell Technologies provides secure decommission and disposal. Before you return the hardware, Dell runs a procedure to ensure that all data on the hardware is inaccessible. Dell decommissions and recycles the hardware by following the industry best practices. Dell's Return Streams Data Security policies and procedures include supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media (including back-ups), ensuring data is not recoverable by any computer forensic means.

Q | How are multiple users managed through the Dell Technologies APEX Console?

A: Simple role-based access control helps you manage what users can see or do within the APEX Console. Only users with appropriate permissions can perform certain actions, e.g., allowing only procurement personnel to place orders, or allowing only senior IT operations personnel to carry out maintenance tasks. The APEX Console also includes an audit log feature that captures identity management actions such as user creation or role assignment.

Q | How secure is Dell Technologies supply chain?

A: Dell Technologies takes a holistic approach to protecting its supply chain and delivering solutions that customers can trust. Our strategy of "defense-in-depth" and "defense-in-breadth" involves multiple layers of controls to mitigate threats that could be introduced into the supply chain. These controls, along with effective risk management, help establish supply chain security.
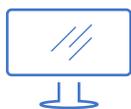
Learn more about
APEX Cloud Services
with VMWare Cloud at
www.DellTechnologies.com/
SimplifyMulticloud

Contact a
Dell Technologies
Expert

View more
resources

Join the conversation
with #DellTechAPEX

D∕ELL Technologies

A P E X