Lenovo

Lenovo ThinkAgile CP Security (Technical Brief)

Models: CP 4000, CP 6000

Note

Before using this information and the product it supports, be sure to read and understand the safety information and the safety instructions, which are available at the following address:

http://thinksystem.lenovofiles.com/help/topic/safety_documentation/pdf_files.html

In addition, be sure that you are familiar with the terms and conditions of the Lenovo warranty for your solution, which can be found at the following address:

http://datacentersupport.lenovo.com/warrantylookup

First Edition (March 2020)

Contents

Security in ThinkAgile CP

The ThinkAgile CP Composable Cloud Platform is a hardware and software private cloud appliance placed inside a customer's data center and managed from a cloud portal running on AWS.

This topic describes the powerful security features in ThinkAgile CP, including role-based access control (RBAC), two-factor authentication, secure multi-tenancy, use of up-to-date and secure application templates, application-level micro-segmentation, and FIPS-compliant data-at-rest encryption, combined with a Security Development Lifecycle (SecDL) and regular penetration testing that is integrated into product development.

A Quick Primer on ThinkAgile CP Abstractions

Understanding some of the main ThinkAgile CP concepts and abstractions will be useful to understanding how ThinkAgile CP security works.

We briefly describe these key abstractions first:

- A migration zone (MZ) is a set of compute nodes among which an application (VM) may migrate. Compute nodes (and applications that run on these nodes) can be assigned categories and tags. Together, categories and tags are called compute constraints. An app will only be allowed to run on a node with the specified compute constraints, i.e. the specified category and specified tags.
- Storage is grouped into storage pools (SPs) for administration purposes. Storage pools consist of storage blocks. A storage block is a pair of storage controllers and all storage accessed through those two storage controllers.
- Finally, a Virtual Data Center (VDC), which is a pool of logical resources, is assigned to a tenant of the ThinkAgile CP Cloud Platform. The logical resources for a VDC may come from one or more MZs and one or more SPs. Applications (VMs) are provisioned inside VDCs.

ThinkAgile CP Security Features

Security features of the ThinkAgile CP Platform are described below.

Refer to the following features:

- “Data Protection” on page 2
- “ThinkAgile CP Hypervisor” on page 2
- “Lenovo Cloud Marketplace” on page 2
- “Micro-segmentation” on page 2
- “Security Testing” on page 2
- “Security Development Life Cycle” on page 2
- “Multi-tenancy” on page 3
- “Secure SaaS Portal” on page 3
- “Built-in Security Monitoring” on page 3
- “Role-based Access Control” on page 3
- “Web Services API” on page 3

Data Protection

ThinkAgile CP provides strong data protection by encrypting all data at rest with FIPS 140-2 encryption. The system supports key management through the built-in hardware security (TPM) module and, if desired, by using external industry-standard Key Management Interface Protocol (KMIP) key management servers such as Vormetric and Safenet. For more information, see Manage encryption.

Every storage block is protected with a 512-bit key that can be changed at any time by the customer. We use software encryption that is performed in the storage controllers and meets HIPAA, PCI DSS and SOX standards. We use Advanced Encryption Standard or AES encryption in xts mode. Furthermore, we use the sha256 hash to convert user-supplied passphrases into keys. By using Intel CPUs with AES-NI support in our storage controllers, we can get between 2-3 GB/s of performance for our software encryption.

ThinkAgile CP Hypervisor

The ThinkAgile CP hypervisor is the RHEL 7 hypervisor with all the latest patches from Red Hat applied. Our hypervisor provides security certifications, such as common criteria certification at EAL 4+, FIPS 140-2 and USGv6. Customers do not have to worry about patching the hypervisor to its latest level, because we automatically push the latest updates and security fixes from our cloud portal to the customer equipment on-premises. For privacy reasons, we do not automatically update the customer's VMs as we do not know or wish to know what they are running inside the VMs. That is the user's responsibility.

Lenovo Cloud Marketplace

Included with the ThinkAgile CP platform is an application marketplace (Lenovo Cloud Marketplace) that comes with a set of ready-to-deploy apps. We allow for simple point-and-click deployment of applications in the Lenovo Cloud Marketplace. ThinkAgile CP automatically updates and patches the application templates in the Lenovo Cloud Marketplace to be up-to-date and also runs virus scans against them to eliminate vulnerabilities. If you deploy an application template from the Lenovo Cloud Marketplace, they can be assured the template is up-to-date and virus-free as of the time of deployment.

ThinkAgile CP also supports private marketplaces, but customers will have to download the latest version of templates from the Lenovo Cloud Marketplace to be sure they have the latest updates and security patches.

Micro-segmentation

The ThinkAgile CP platform supports true micro-segmentation using a combination of overlay networks, distributed firewalls and per-application firewall overrides. This enables zone defense on a per application basis, thereby containing the effects of any application exploit to only the micro-segment on which it occurred. Each micro-segment is completely isolated from all other micro-segments.

Security Testing

Every major release of software is regularly penetration tested by the well-known external security audit team from Net Square Solutions. Both the on-premises software and the SaaS portal code are penetration tested. In this way, software vulnerabilities, as well as our incident management procedures are regularly tested.

Security Development Life Cycle

The ThinkAgile CP security development life cycle integrates security into every step of product design and development, rather than applying it as an afterthought. The strong pervasive culture and processes built around security harden the ThinkAgile CP Composable Cloud Platform. For example, research and development teams work together to fully understand all the code in the product, whether it is built in-house or inherited from dependencies. Strict tests for Common Vulnerabilities and Exposures (CVE) are built into the product QA process, and updates to handle known CVEs are scheduled for minor release cycles to minimize zero-day risks without slowing down product evolution. Other practices include regular penetration testing, limiting every user to the fewest privileges needed based on their role, use of 2FA for all cloud accesses, logging all admin accesses, ensuring all software and templates are always kept up to date, and limiting access to encryption keys which are customer controlled.

Multi-tenancy

We provide secure multi-tenancy, allowing multiple tenants to run fully isolated from each other on our platform. The multiple tenants can be given separate hardware if so desired. Even when multiple tenants share the same hardware, application level micro-segmentation (as previously described) is used to isolate the applications of the different tenants.

Secure SaaS Portal

A secure SaaS portal manages the ThinkAgile CP platform. The SaaS portal does not require the customer to open any inbound firewall ports, as all communication is initiated by the ThinkAgile CP platform in the customer data center. All outbound communication from the customer data center to the SaaS portal uses TLS encryption, and we use a standard SSL handshake to authenticate with the portal, before sending any data out. Every piece of ThinkAgile CP software at each customer's site has its own separate identity. The portal, once it authenticates software from customer X, will only allow that software access to data related to customer X. All hardware at every customer site has to be registered with our portal, to prevent hardware spoofing.

Built-in Security Monitoring

ThinkAgile CP has built-in security monitoring for suspicious activity and it has remediation procedures for when such activity is detected. An example of a suspicious activity being monitored is hardware known to the portal to have failed but still talking to the portal. We will continue to enhance the list of suspicious activities to be monitored as needed.

Role-based Access Control

Our platform enforces Role-Based Access Control (RBAC) for system administrators. ThinkAgile CP supports four roles in all. It supports two management roles - an infrastructure admin role for managing the physical infrastructure and a separate VDC manager role for people managing the virtual datacenters and applications. In addition to the two management roles, ThinkAgile CP also supports two viewer roles - these are roles that can see things but cannot take any actions. There is an infrastructure viewer role (with visibility similar to the infrastructure admin role) and a VDC viewer role (with visibility similar to the VDC manager).

Two-factor authentication

ThinkAgile CP uses two-factor authentication (2FA) security measures to prevent unauthorized access to user accounts in the SaaS management portal. By requiring more than one factor during the authentication process, there is increased assurance the user’s access is authorized. The platform enforces two-factor authentication and it requires the following details before allowing access to user accounts:

1. Enter username and password to log into the account
2. Validate the login by entering a security code received via mobile phone or e-mail

Web Services API

To support programmatic management of our platform, ThinkAgile CP supports a Web Services API called CPWS (ThinkAgile CP Web Services). The API supports actions against applications, application groups, application templates, migration zones, storage pools and virtual networks . API access is over https to ensure privacy, and a security token is needed to access the API.

Lenovo