Because IBM Cloud Private is built with a security mindset, all application management interfaces and data handling are accessible from within only an organization security zone in accordance with the organizational requirements in place.

Because IBM Cloud Private includes a portfolio of Cloud-ready applications, the deployment of such an infrastructure is more secure than traditional on-premises infrastructure. This occurs because by using IBM Cloud Private, customers can apply uniform security policies across all applications within its simple management interface instead of traditional on-premises infrastructures that rely on manual updates to each service on top of a stack of applications.

Application Security

Vulnerability Advisor is a feature of Cloud native and Enterprise editions of IBM Cloud Private to retrieve security status for container images on top of the IBM Cloud Private registry. It also checks for the security and compliance status of running containers that are deployed within an infrastructure. Vulnerability Advisor can also be configured to scan private registries to ensure that even customer-owned images are scanned for potential security threats.

Such a feature allows for customers to quickly assess and address possible security threats and act on their remediation quickly. It is also possible to review security reports with ease directly from the IBM Cloud Private management interface.

Vulnerability Advisor security notices are reviewed, processed, and made available by IBM Security to ensure that customers receive potential threat reports in time about their managed infrastructure, which greatly reduces potential intrusion threats with ease.

Note: For more details on Vulnerability Advisor, see Managing image security with Vulnerability Advisor

Service IDs and API Keys

One of the growing concerns of cloud applications and microservices-based workloads is how each component of an application is communicating with each other and how secure are such credentials that are propagated within the network. Moreover, another important factor to consider is how services or applications that are outside of the on-premises cloud infrastructure can interact with it.

IBM Cloud Private allows for developers to further use their cloud applications by using Service IDs and API keys. Service IDs identify an application or service; API keys are used as an authentication method for such Service IDs.

By creating specific Service IDs and their respective API keys, developers can use credentials that use the principle of least privilege. That is, it allows connecting applications to be granted access only to the minimum set of information that is required for its legitimate purpose and functioning.

Service IDs are not tied to a particular user in such a way that if a developer leaves the organization, the service ID remains, which ensures that the application or service in question continues to operate.

Also, by creating individual credentials for each service, if an API key is compromised, it does not give access to other resources across an infrastructure. IBM Cloud Private allows for the quick replacement of lost API keys across its infrastructure in such a way that credentials can be quickly refreshed by using the IBM Cloud Private management interface.