The roles discovery and CMDB play in asset management

How automated discovery and configuration management support asset management and software compliance

Benefits

- Get better use of IT assets and fewer software licensing violations
- Discover software installed on cloud or inside containers
- See how IT assets deliver business services for better decision-making
- Gain a comprehensive view across IT environments, endpoints, and devices

Enterprise technology managers need to understand the infrastructure, devices, and software their organization uses, how it is configured, and the role each element plays in supporting their business processes. This is essential to asset management, reliability, security, software compliance, and in some cases, regulatory compliance.

However, this seemingly simple goal is difficult to achieve in practice. In addition to on-premises servers, networking devices, and endpoints, organizations now use a plethora of Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) solutions from cloud providers, such as Amazon Web Services, Google Cloud, Microsoft Azure, and Oracle Cloud. Employees are also using their own devices more often, blurring lines between employer and staff assets.

In the software arena, on-premises installations are now used alongside Software as a Service (SaaS) products. Software is also residing within virtualized containers and enterprises are accessing it as a microservice, sometimes for very brief periods.

The need for a new approach to discovery and CMDBs

These fundamental changes must be met with equally significant changes in the tools used to understand an organization's information technology environment. In terms of asset management and software compliance, this means rethinking approaches to discovering items within an environment and using configuration management database (CMDB) tools to capture that information and make it available to teams across the organization.

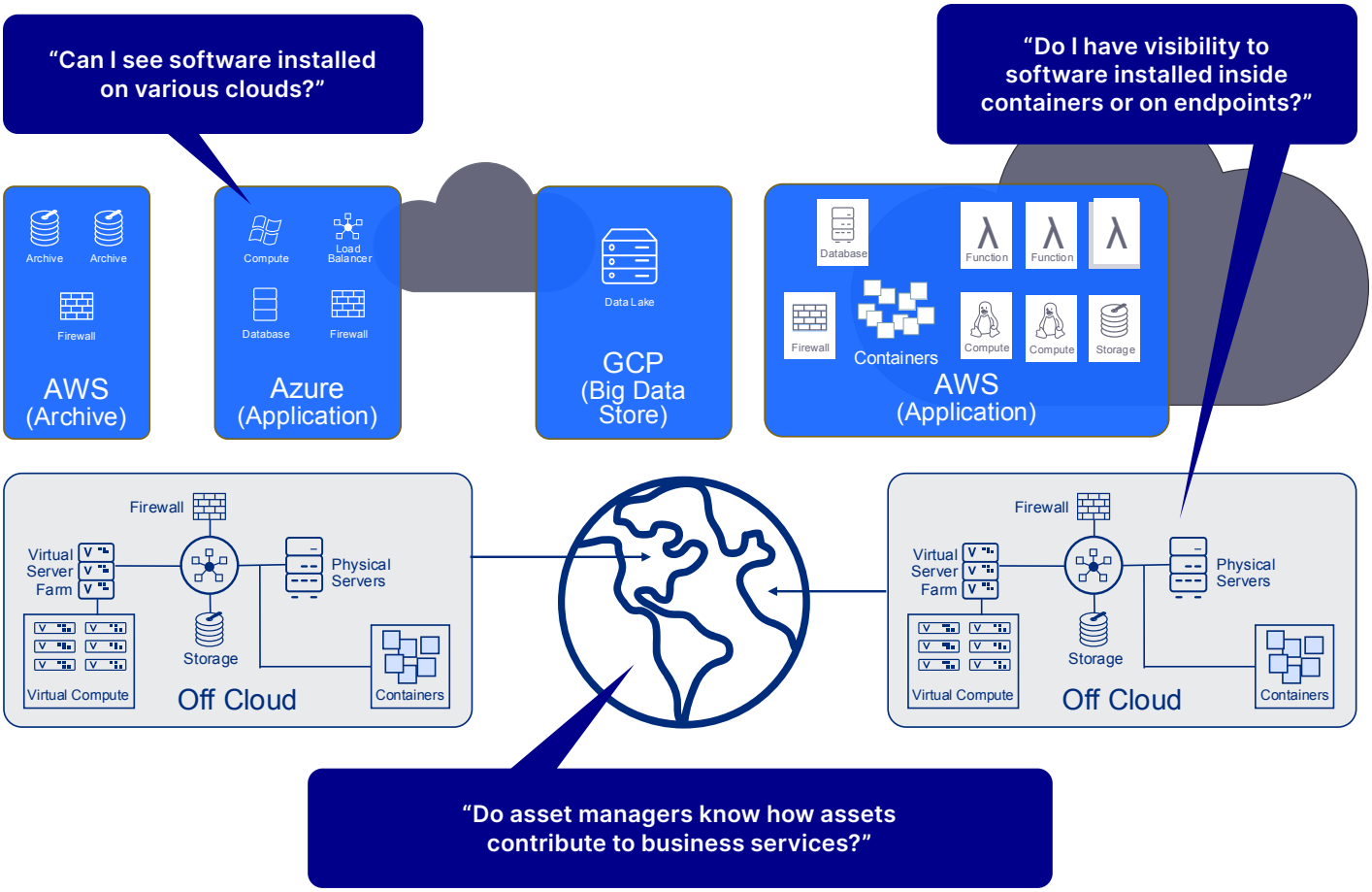
This requires a centralized solution that provides a single, clear, and constantly up-to-date view of IT assets across hybrid or multicloud environments and should feature the following characteristics.

Comprehensive and penetrating

Discovery tools enable managers to map the assets being used within their environment automatically and regularly. To achieve this, they need to be able to recognize an enormous range of infrastructure and software across on-premises and cloud environments, and in conventional and virtualized domains.

For example, OpenText's discovery solution can identify networking equipment from more than 250 vendors and 3,500 network devices. This enables detailed Layer-2 discovery of physical and virtual networking components, including software-defined networking, firewall, and wireless items. The solution can also recognize close to 140,000 software applications, including those held within containers and many older ones that might have been installed years earlier or introduced due to an acquisition.

Such comprehensive coverage is essential to identifying non-compliant or misconfigured infrastructure assets, and outdated or vulnerable software.



Considerations for the role discovery plays in asset management

CIOs should be alarmed that 53% of IT teams lack complete visibility into technology assets.

Flexera 2024 State of ITAM Report ›

Centralized and integrated

An effective discovery and CMDB solution should act as a single, centralized, and vendor-agnostic repository of asset information. But it should also enable specialist teams to use their preferred monitoring and management tools in areas such as service management, networking, applications, and cybersecurity. This can be achieved through integrations with those specialist tools and application programming interfaces to enable customized integrations with other products.

Automated, efficient, and cost-effective

By automating discovery, organizations can maintain a real-time view of their assets and configurations, even as changes are made and other events occur. For this to be effective, however, the discovery and CMDB solution must be able to navigate security constraints and network requirements, and work across compute platforms. It should also support both agentless and agent-based discovery, such that the centralized solution can gain input from scans of the environment and information sent from software agents installed on equipment.

In addition, discovery solutions should be efficient. For instance, they should complete incremental updates to capture changes—rather than generating larger network loads—by periodically creating new records across an entire environment. They should also know the IaaS and PaaS used in third-party clouds without needing extra discovery licenses.

Aligned with vendor licensing tools and frameworks

Having an ongoing and accurate view of the software assets being used by an organization is essential to ensuring compliance with licensing requirements. It can also greatly reduce the time and effort needed to respond to software vendors' audit demands.

These benefits are enhanced even further if an organization's discovery and CMDB solution aligns with the licensing tools used by software vendors. For this reason, OpenText has built its discovery and CMDB solution to align precisely with the licensing tools and frameworks used by major vendors, along with the ability to create your own discovery to identify home-grown or highly specialized software outside the scope of traditional software discovery signatures.

Aware of the relationships between assets and service delivery

Finally, an asset management solution should play a key role in ensuring business processes remain up and running. In addition to identifying old, non-compliant, or misconfigured items that could undermine stability, it should help the organization know the role and value of each asset. This is achieved by mapping assets to services and then considering those insights when maintaining or changing the assets.

This elevated level of service awareness will also support compliance with regulations such as the European Union's Digital Operational Resilience Act (DORA). This requires organizations to understand who and what will be affected if incidents, changes, vulnerabilities, or outages occur in delivering their digital services.

Resource

Learn more about OpenText Universal Discovery and CMDB and the role discovery can play in other areas of IT operations ›

OpenText Universal Discovery and CMDB

OpenText adheres to these principles with OpenText™ Universal Discovery and CMDB—a vendor-neutral configuration management solution, deployed as SaaS, on-premises, or in the cloud. OpenText Universal Discovery and CMDB automatically collects (by discovery or seamless integrations with IT tools and platforms already in place), reconciles, manages, and presents configuration items for hardware, software, applications, services, and their interdependencies across on-premises and multicloud IT environments. The result? Your IT landscape snaps into sharp focus, empowering you to increase security and compliance.

opentext™