The roles discovery and CMDB play in compliance and security

How configuration management increases IT governance and security

Benefits

- Better use of IT assets and fewer software licensing violations
- Faster incident identification and resolution times
- Accurate, real-time configuration information across IT
- Comprehensive view across IT environments, endpoints, and devices

While advancements such as digital transformation, outsourced and hosted services, and ever-expanding integrations have delivered many benefits, they have left organizations with far more complex and opaque systems.

This creates challenges for both IT managers and the business leaders who rely on these systems. Without a central repository that can provide a clear and comprehensive picture of infrastructure, configurations, and installed software across all environments, they risk breaching software licensing conditions, being exposed to software vulnerabilities, and failing to comply with regulations.

An accurate CMDB is critical to compliance

One reason organizations are struggling to manage their sprawling IT environments is that their use of configuration management databases (CMDBs) and discovery methods has yet to keep pace with their digital transformations.

CMDBs are critical because they enable organizations to understand the myriad parts of their IT systems and how they interact with each other. However, their effectiveness is often undermined by organizations using too many of them. Teams too frequently manage parts of technology systems—such as servers, software applications, and networks—using discovery tools that are specific to their areas only.

With siloed discovery approaches and systems, organizations don't have a complete view of their environment, which is critical for compliance.

Nearly one quarter of global IT leaders reported they paid more than $5M in audit costs over the last 3 years.

Flexera 2024 State of ITAM Report ›

Considerations for the role discovery plays in compliance

Another issue is the use of discovery and CMDB tools that do not provide enough information for a truly comprehensive view of the IT system.

This can be problematic, for example, when incidents such as Log4j occur, when it was discovered that hackers could use a very common, free logging framework to access systems and cause significant damage. Many organizations were left exposed, as it took considerable time to identify whether and where they use the software, as it resides within a library, making it harder to spot.

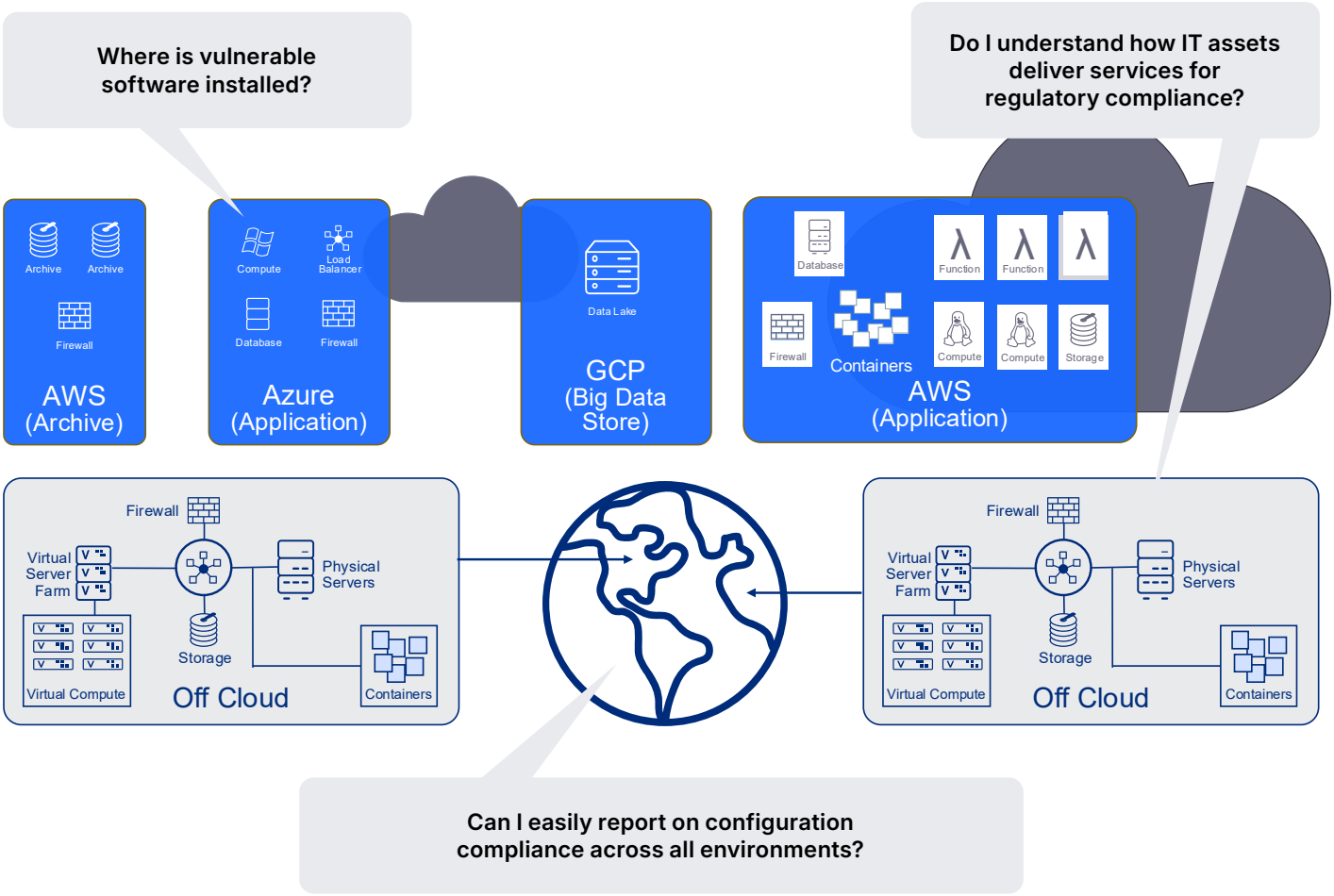
Similarly, organizations can have poor visibility of software applications running inside containers at third-party cloud providers. This can create security vulnerabilities and commercial issues if organizations discover they aren't paying for the software licenses they should be.

Many organizations also lack a clear understanding of their core IT assets. For instance, they cannot say how many servers, switches, and laptops they own. Nor can they say how these assets are configured, how old they are, and what role they play in their operations.

This of course is required information for an organization, however understanding the value of each of these assets is crucial to compliance. While all are equal on paper, a switch delivering network connectivity for a payment processing system will be of greater value to the organization than one sitting redundant in a development lab. What equipment does and how services are delivered can now also be critical in compliance reporting.

For example, the European Union's new Digital Operational Resilience Act (DORA) requires financial institutions to have a high level of understanding of their IT systems, such that they can say who and what will be affected if incidents, changes, vulnerabilities, or outages occur in the delivery of their digital services.

Organizations often also struggle with challenges arising from other new regulations, such as assuring all databases are encrypted to ensure compliance with Europe's General Data Protection Regulation (GDPR) information privacy rules. Or ensuring that the cloud computing services they use comply with security requirements under the United States Government's new Federal Risk and Authorization Management Program (FedRAMP).



Considerations for the role discovery plays in compliance

Operate on the strongest foundation—complete and scalable discovery

Meeting these challenges—and ensuring any system is compliant and secure—relies on an effective discovery and CMDB solution.

The central guide provided by such a solution is essential for any organization that wants to swiftly identify misconfigured or noncompliant infrastructure, and outdated or vulnerable software, to reduce compliance and security risks in complex environments.

To achieve this, an effective CMDB solution requires the following key elements.

Comprehensive

A CMDB should be able to easily discover, map, and manage configuration items across an organization's entire IT environment. Today, that means spanning infrastructure and software spread across on-premises systems, multiple clouds, and work-from-anywhere devices. It also means being vendor-neutral, such that the CMDB works with varied equipment, software, and all the other IT management tools an organization relies on.

Resources

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

Agent-based and agentless

Agents are software installed on devices, such as laptops, that report information back to a server. Discovery solutions can also be "agentless," meaning they rely on scanning activity to discover the hardware and software contained in an environment. Both approaches are important for organizations to maintain a comprehensive view of their environments that is updated in real time as changes occur.

Automated and penetrating

A modern CMDB should provide reliable and automated discovery across any security constraint, network requirement, or computing platform. To address the challenge of identifying all the software used in an environment, CMDB solutions should be capable of full software discovery and utilization across all devices and environments—including cloud, containers, and endpoints.

Deployment flexibility

Organizations often need deployment flexibility to be compliant with IT, networking, or security policies. However, discovery and CMDB solutions have historically been either on-premises or exclusively SaaS-based solutions, often limiting how the CMDB can be used. A modern discovery and CMDB solution should offer various, secure deployment options, ranging from on premises to public or private cloud—including approved in-country clouds and government-approved clouds, to meet various regulatory requirements.

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 multi-cloud IT environments. The result? Your IT landscape snaps into sharp focus, empowering you to increase security and compliance.

opentext™