vArmour

SOLUTION BRIEF

Reconcile CMDB Data to Improve Enterprise Decision-Making and Service Quality

Poor CMDB Data Quality Holds Many Enterprises Hostage

Within enterprises, few business leaders believe the data from their CMDBs is accurate or complete. There are many reasons for this troubling state of affairs, where error-prone data is common and persists:

- Outdated records from process or accountability gaps in operations teams
- Out of sync records in multiple CMDBs due to dynamic changes, new cloud infrastructure, and new applications
- Conflicting or siloed data in multiple CMDBs from mergers and acquisitions
- Inaccurate records from manual or incomplete audit processes

The most visible negative impact of poor CMDB data quality is unplanned or self-inflicted downtime and delayed service restoration when changes are made and errors are unanticipated. Besides damaging customer satisfaction, poor IT performance and availability also has a significant and real cost to the bottom line. For example, recent research shows that a single hour of downtime costs $300,000 or more for over two-thirds of all businesses. [1]

More importantly, poor CMDB data quality can negatively impact the speed and quality of business decision-making. Issues in managing change mean that enterprises cannot achieve their key strategic initiatives like digital transformation, cloud migration, and Zero Trust security, or even much smaller tactical operational projects. Finally, unmanaged or stranded corporate assets can drain operating budgets due to unused assets, maintenance and support fees, and data center costs, without providing any business benefit at all.

In 2020, 32% of Gartner inquiries regarding IT service view CMDBs cite data completeness or quality concerns as a challenge. Through 2024, 99% of organizations using CMDB tooling that do not confront configuration item data quality gaps will experience visible business disruptions. [2]

Discover and Inventory Applications and Assets to Reconcile CMDB Data

Enterprises can benefit from new and modern application discovery tools from vArmour in an emerging category, called Application Relationship Management (ARM). These solutions can see into and across heterogeneous data center and cloud environments; ingest, aggregate and correlate real-time telemetry data from disparate underlying platforms; and then visualize and inventory all the applications, workloads, users and relationships accurately and continuously.

With these insights from understanding application relationships and dependencies, enterprises are able to now pursue multiple use cases that deliver value in previously unachievable ways.

What is different from existing tools is that vArmour does not require the deployment of new infrastructure - no new agents, appliances, or architectures - and organizations can leverage the investments they already have in place. As a result, organizations can begin to realize value from enterprise-wide visibility within days.

Implementing vArmour solutions throughout the lifecycle, including auto-discovery, continuous

monitoring for change validation and alerting, and long-term reporting, will increase the accuracy of the CMDB data while reducing the time spent by every application owner across the organization.

[1] ITIC, Hourly Downtime Costs Rise: 86% of Firms Say One Hour of Downtime Costs $300,000+; 34% of Companies Say One Hour of Downtime Tops $1 Million, May 2019.
[2] Gartner®, 3 Steps to Improve IT Service View CMDB Data Quality, Roger Williams and Kenneth Gonzalez, 9 December 2020.

Auto-Discovery: Provide automated discovery of application relationships and dependencies, so organizations can detect, describe, maintain and validate each unique dependency based on environment telemetry.

Continuous Monitoring: Enterprises can deploy continuous monitoring for environment changes, understanding whether changes are within approved scopes or require attention as well as monitoring communications against the approved model, alerting on any deviations from normal.

Long-Term Reporting: Long-term monitoring of dependency utilization can also facilitate annual attestation and removal-of-state approvals. Unlike many tools, vArmour can handle the recording, storing, and analyzing of historical communications over time to account for seasonal and periodic dependencies; then deliver annual reports as a part of annual dependency attestation processes.

The Benefits of Application Visibility for CMDB Reconciliation

With complete visibility of all applications, workloads, assets, and their relationships, enterprises can begin to reconcile their CMDBs to improve and update outdated, inaccurate and conflicting records. Accurate CMDB data can then enable organizations to realize significant value during change management in gaining this enterprise-wide visibility by helping to improve the operational efficiency and cost of the application infrastructure, as well as strengthen their cybersecurity posture.

For example, IT operations can decommission unused, redundant, or stranded assets that have accumulated over time or due to acquisitions. This also can reduce the risk of vulnerabilities from a smaller threat surface area. And with a more accurate understanding of their IT infrastructure, enterprises can automate more processes and tasks with confidence.

A common hurdle IT faces is that different stakeholders want to keep these assets operational, asserting their continued use. vArmour can actually prove whether or not any users or other workloads are actually using these applications. This real-world visualization of relationship data can help organizations prioritize their decommissioning projects and communicate effectively to any impacted users.

In addition, a more complete and accurate picture of IT infrastructure enables compliance teams to more easily meet regulatory reporting requirements for IT asset audits and dependency mapping. Finally, organizations can create and deploy more effective cybersecurity policies based on actual user and application behavior that will replace the flat corporate networks in place and enforce secure micro-perimeters around all applications and assets that align to Zero Trust security principles.

The Time Is Now

When important business data is inaccurate or incomplete, enterprises cannot begin to achieve their mission-critical objectives by delivering services to market faster and making well-informed decisions. vArmour is devoted to helping businesses solve these challenges effectively, efficiently, and securely. See what you've been missing.