vArmour

SOLUTION BRIEF

Reduce Your Operational Risk With Better CMDB Data Quality

Lack of Visibility Can Result in Damaging Attacks and Service Outages

A core mission of IT organizations is to ensure applications are available and secure. That starts with a good understanding of their IT estate. However, most business leaders don't believe the systems of record that store their asset and application data, called CMDBs, is anywhere close to accurate or complete. In many cases, information in CMDBs is filled with inaccurate, outdated, or incomplete data. Environments change constantly and CMDB records can't keep up.

There are many reasons for this situation. Standard processes don't exist or aren't followed, accountability isn't clear or prioritized, and manual audit procedures are too burdensome and error-prone. Operations teams have no automated solutions to ensure accuracy.

The impact of this lack of visibility is damaging and disruptive to many organizations. Enterprises incur additional security risks from vulnerabilities to unknown and unpatched workloads, unused assets that increase the attack surface area, and hidden dependencies between applications that can let attackers move laterally within the network. Organizations also suffer costly unplanned downtime when changes are made that unexpectedly break critical services. 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]

Given most businesses are accelerating their digital commerce, this problem can only get worse without a fundamentally new approach.

Find Applications and Assets Dynamically to Improve Resiliency and Security

Enterprises need an automated and dynamic way to find and inventory all their assets and applications, wherever they're located. vArmour provides a solution that helps organizations identify all the applications, assets, and users across their complex hybrid cloud environments in a new and modern emerging category, called Application Relationship Management (ARM). vArmour's ARM solution improves an organization's operational resiliency and security posture with enterprise-wide visibility. With vArmour, organizations 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.

This enterprise-wide visibility can be used to update systems of record like CMDBs to ensure continuous and accurate information. With more accurate and up-to-date CMDB data, organizations can work more effectively to comply with operational resiliency and risk objectives.

What's more, vArmour discovers and visualizes the dependencies and relationships among applications, assets, and users to provide more insights and understanding of the environment. With these insights, enterprises are now able to identify application dependencies that cause service disruptions during operational changes and increase the risk of breaches to unknown assets.

[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.

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.

Gain Insights Throughout the Application and Asset Lifecycle

Implementing vArmour solutions throughout the application and asset 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. Enterprises gain continuous updates and insights through three parallel processes:

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 on demand.

Greater Resiliency and Security with vArmour

With an accurate understanding of the IT infrastructure, vArmour enables enterprises to ensure greater operational resiliency during change management and strengthen their cybersecurity posture with fewer unknown vulnerabilities. Because vArmour provides enterprise-wide visibility of all applications, workloads, assets, and their relationships, organizations can 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 resiliency during change management and cost of the application infrastructure, as well as strengthen their cybersecurity posture with fewer gaps and unknowns.

For example, IT operations can decommission unused, redundant, or stranded assets that have accumulated over time or due to acquisitions that increase the threat surface area. 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.

With an accurate understanding of the IT infrastructure, vArmour enables enterprises to ensure greater operational resiliency during change management and strengthen their cybersecurity posture with fewer unknown vulnerabilities. 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.