CUSTOMER CASE STUDY

Global Retailer Accelerates Business Unit Separation While Managing Compliance, Risk and Cost

504 APPLICATIONS	5.8M RELATIONSHIPS	84,000 WORKLOADS
MAPPED IN 30 DAYS		

A well-known specialty retailer headquartered in the U.S., but global in scope, has long owned many clothing and fashion brands. After a series of divestitures, however, the company decided to separate its last two brands into publicly traded companies in 2020.

Separation anxiety and challenges

As part of its legal separation process, the company needed to divide its existing IT infrastructure and systems. The IT team wanted to complete this asset segregation within two years. The plan included determining which applications will be moved to different environments, refactored, and/or decommissioned; and in what priority order, all without incurring service disruptions or security breaches.

But first, the retailer had to start with the basics: identifying the systems and users that support only Brand A or Brand B, and those that support both brands. Many of the IT assets and services are shared between the brands in order to maximize utilization and return on investment.

Currently, the retailer has a restricted and incomplete view of all the systems and users within its IT infrastructure, inhibiting its ability to identify systems and users by brands—as well as the relationships and dependencies between them. The retailer's existing approach was to map the applications, users and dependencies via a manual process, which would be costly and too time-consuming as there are 504 applications, 84,000 workloads and 5.8 million relationships, with an average of 69 relationships per workload. To identify the more than 50,000 devices and their relationships or dependencies, for example, was estimated at thousands of person hours and cost more than USD$10 million.

In addition, the retailer's IT infrastructure is a heterogeneous and dynamic environment consisting of physical, virtual and cloud systems -including Microsoft Azure- adding layers of complexity to the manual process. This current solution would return incomplete and inaccurate information, and fail to identify all relationships and dependencies. It would likely result in unplanned service outages and increase security risks during separation.

Why vArmour?

> "Now I am seeing the value of vArmour and how we can use this across the business. It's more than brand separation; we can use vArmour to help enforce what our teams have said they've implemented."

Overview

A well-known specialty retailer is separating its last two brands into two companies

The Challenge

The retailer needed to divide its existing IT infrastructure and systems without incurring disruptions or security breaches. However, the retailer encountered the following problems:

- **No visibility:** Unable to identify systems, users and their relationships by brands
- **Complex environment:** IT infrastructure consists of physical, virtual and cloud systems
- **Inefficient process:** Manual approach to mapping data is costly, time-consuming, and inaccurate

Solution

vArmour Relationship Cloud, a SaaS-based Offering

The Results

- **Reduced cost and time** for separation with full application visibility of 504 applications and 84,000 workloads in just 30 days
- **Lowered risk of security and outages** with 100% visibility of dependencies
- **Maintained accurate data** on IT systems and users
- **Discovered the unknowns** that can lead to hidden security and compliance risks

Solution requirements: application relationship mapping

For the application, user and dependency discovery phase of the separation, the retailer wanted a solution that could fulfill the following requirements:

- Identify all applications, systems and workloads associated with each brand quickly and efficiently
- Identify all users by business unit that access the applications, systems and workloads
- Integrate with their endpoint and workload security solution for policy enforcement
- Minimize outages and disruptions associated with separation, changes and migrations
- Automate the continuous assessment of dependencies and updates to policies post-separation
- Update and automate the reconciliation of the configuration management database (CMDB)

Solution: vArmour Relationship Cloud

The retailer was able to accelerate the project timeline and avoid the deployment of additional on-premises systems during the discovery phase by using vArmour Relationship Cloud, a SaaS-based offering.

vArmour automatically discovers and visualizes application, user, region and realm relationships, dependencies and communications across a heterogeneous environment without requiring incremental agents. The reporting is customized to tell how many users from which brand are (or are not) accessing the applications, and which applications are communicating with each other. With this, the retailer can determine timing and priorities for application refactoring and moving.

vArmour baselines performance and policies before the move or refactor, and applies the same policies afterwards. These policies can be simulated before enforcement to reduce security gaps and vulnerabilities. The continuous assessment of applications and dependencies post-refactoring and post-separation updates dependency baselines and security policies.

The ability to sync with IT service management and cybersecurity asset management platforms allows the retailer to update the CMDB by observing application traffic. This helps the retailer to establish a dynamic and data-driven inventory of all assets and user interactions on the network.

Results: Retailer accelerated separation process with reduced cost

With vArmour as a strategic partner, the retailer was able to plan the division of its IT systems with full visibility and confidence, and benefit from the following:

- Reduced cost and time for separation with full application visibility of 50,000 devices, 504 appllications, 84,000 workloads with 5.8M relationships in only 30 days; and automation for continuous assessment of systems, updated security policies, and systems data reconciliation for separated brand financials.
- Lowered risk of outages with 100% visibility of application dependencies for refactoring and moving. Policy simulation and monitoring reduced security gaps and vulnerabilities.
- Maintained accurate IT systems and user data via continuous CMDB reconciliation with other platforms.
- Discovered the unknowns that can lead to hidden security and compliance risks. In one instance, vArmour discovered an application that was unknowingly polling the entire network violating existing governance and compliance policies. Hundreds of retired servers were discovered to still be running. In another case, vArmour identified a potential breach of sovereign data leaving the country, violating existing governance policies.

Find out more about vArmour

varmour