PRODUCT OVERVIEW

vArmour Data Flows Module

Transformative visibility of data flows through middleware

Digital services are imperative for every modern business and must be highly available and secure. Many legacy and modern applications are interconnected through middleware, such as messaging queues (MQs) and FTP servers which form the communications heart of the core business. Costly and disruptive service outages happen regularly when applications are updated, patches are deployed, and changes are made. Security breaches quickly become more impactful and difficult to remediate when the attack path cannot be identified easily.

Challenge: Serious blind spots due to middleware

Many enterprises suffer escalating resiliency and security issues without the ability to understand what's causing the problems in the first place. Their highly interconnected applications and data - a prerequisite for modern business - are more complex, voluminous and distributed than ever before. A huge complicating factor is that the middleware integrating these applications together can mask your understanding of application dependencies and data flows, leading to serious blind spots. This inability to track data flow relationships results in hidden cyber risk from a vulnerable attack surface and unknown points of failure.

Existing approaches can't decipher this complexity or easily solve for the blind spots because they are too manual or cannot see through middleware systems.

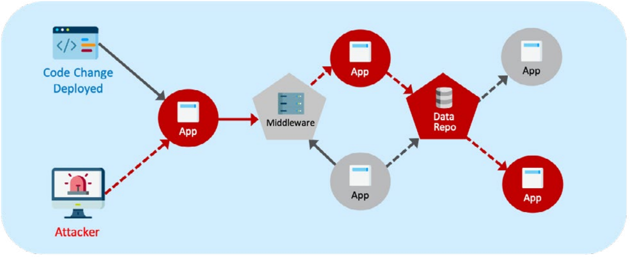

Figure 1: Unknown data flow relationships traverse through app integration layers

Enterprises can't answer foundational questions such as:

- How do you understand and limit the blast radius of a ransomware attack?
- How do you ensure applications are available if others are changed or suffer an outage?
- How do you meet compliance requirements for new regulatory controls?

As a result, enterprises rely on costly manual processes with spreadsheets or struggling to stitch together data from multiple siloed tools. The result is higher cyber risk and costly service outages.

vArmour Solution: Continuous visibility of data flows through middleware

vArmour provides visibility from on-premises data centers hosting legacy applications to public cloud instances hosting modern cloud-native applications. You can see applications, relationships and data flows between middleware within environments as well as across hybrid cloud environments. With its intuitive user interface, you can filter by environment or see dependencies between regions, to get the information you need, fast.

vArmour integrates with underlying platforms to receive and correlate data telemetry in real-time so you have a continuous view of your application environments and the communications behavior between applications.

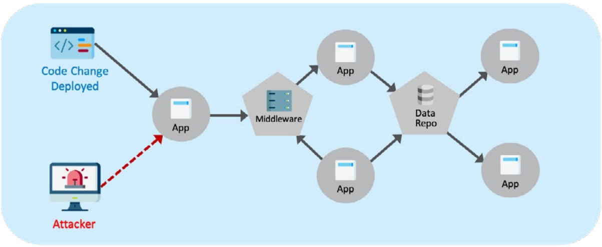

Figure 2: Enrich your understanding of complex relationships through middleware in every environment

Reveal and visualize multi-hop dependencies and data flows through middleware

With the new Data Flows module, vArmour can uncover the hidden multi-hop dependencies and data that flows to and through middleware that increase the blast radius for enterprises across their critical applications when cyber attacks and outages happen.

vArmour helps enterprises to discover and observe the complex application relationships and data that flows through middleware in every environment. Enterprises gain a multi-dimensional view and better understanding of these dependencies. Data Flows can also uncover which applications are producers of data (what is published) to middleware and which applications are consumers of data (what is subscribed).

Implement new security controls

Because of this new understanding of the dependencies and data flows across their IT infrastructure, organizations can limit the extent of any potential damage by implementing security controls to reduce the incident blast radius and by simulating resilience impacts during change management.

Improve compliance reporting

Since regulators have recently recognized the importance of data flow visibility for risk management through new advisory controls, most notably in NIST and SWIFT mandates, enterprises can now meet these new compliance mandates without the costly, time-consuming and manual approaches.

Data Flows Module Product Features

Cyber Asset and Workload Discovery

- Continuously discover and visualize all assets and workloads from existing infrastructure data with a centralized ML-based relationship mapping engine
- Leverage IT and business metadata to correlate into intuitive business centric enterprise side view of applications and their relationships

Continuously Discover Data Flow Relationships

- Visualize data flows and understand dependencies through middleware like IBM MQ
- Enrich understanding of complex end-to-end relationships in every environment
- Understand multi-hop dependencies to limit the blast radius of ransomware
- Align recovery objectives of apps through middleware to improve resiliency
- Document data flows to comply with new regulatory controls

Single Relationship-Based View

- Present a single application-centric and relationship-based view across enterprise IT
- Intuitive user interface for understanding risk, attack surface, and blast radius with enterprise-, environment-, and app-level views
- Drill down into applications to see observed, attempted, and synthetic relationships and baseline behavior in real-time and over time
- Continuously updated relationship graph for discovering, observing, and controlling every application, workload, user access, and data relationship in your environment. Visualize by region, known CVEs, traffic and connections.

API-Based Integrations

- Integrate easily via APIs (and no agents) with common sources of business, IT, & security data — networking, cloud, identity, middleware, and ITSM platforms
- Continuously ingest telemetry data across a broad set of platforms in existing IT infrastructure, from on-premises systems to public cloud domains
- Leverage a standard API connector framework to extend support for new and diverse platforms

Fast Intuitive Search Results

- Query stored data in the relationship graph (or attack surface inventory) data using Relationship Search with flexible, natural language search terms
- Instantly returns intuitive and actionable results that help pinpoint critical application relationships and risks across heterogeneous environments
- Benefit from high performance searches that are 5-10X faster than alternatives

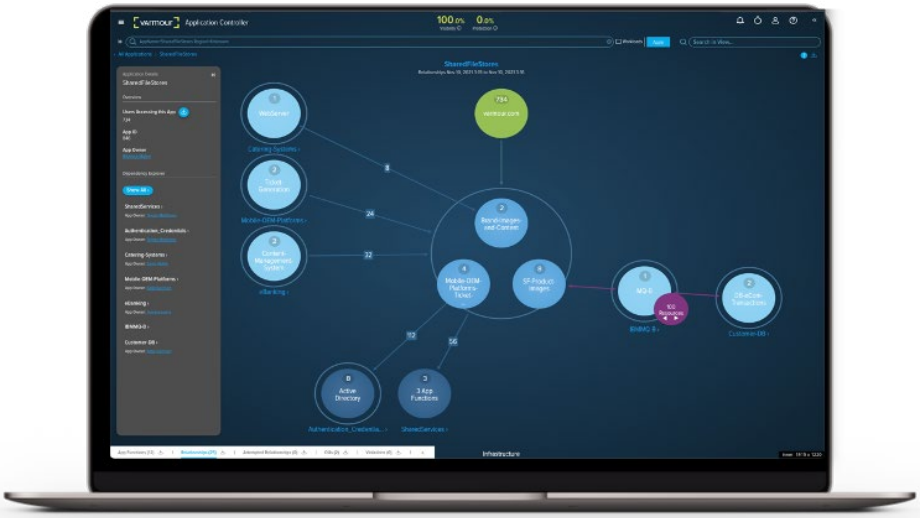

Figure 3: Discover, observe and control the relationships of applications, users, devices and data.

Key Benefits of Data Flows Module

vArmour provides automated, continuous discovery and end-to-end view of multi-hop application relationships and data flows through middleware with important positive business outcomes:

Easier, quicker compliance with regulatory controls

- Understand operational risk for applications interconnected through middleware

Stronger security protections

- Understand lateral attack vectors in the network to minimize the blast radius of attack surface

Higher Services Resiliency

- Validate recovery time objectives (RTOs) and prevent unplanned outages

Faster, more confident change management

- Simulate and analyze the results of changes beforehand to meet new regulatory requirements

Demonstrate faster, easier compliance with new regulatory controls for data flows

- Automated attestation of data flows through middleware

> “Without understanding the upstream and downstream from middleware, we would not get an accurate view of the end-to-end flow.”
>
> – Managing Director, Technology,
> Major U.S. Bank

To learn more, visit www.varmour.com