vArmour

SOLUTION BRIEF

Application Relationship Management (ARM): An Overview

Executive Summary: Application Relationship Management (ARM) is an emergent software category designed to solve contemporary security, risk, and operational challenges now prevalent due to the growth of the "digitally defined" enterprise; the proliferation of software applications, devices, and users; the growing complexity of how these applications are deployed in cloud and hybrid cloud deployment environments; and how users access these applications.

Enterprises are Becoming "Digitally Defined"

Modern "digitally defined businesses are now reliant on connecting people and software applications. For many, this is a defining source of operational and competitive advantage. Enterprises have hundreds or even thousands of applications that are deployed in cloud and hybrid cloud environments, across disparate architectures, technology platforms, networks, and services. Accordingly, IT and security operations are now more dynamic than ever. Applications are added, enhanced, or decommissioned frequently; workloads spun up and down; development and DevOps teams push out production code practically on demand. Increasing numbers of people on myriad types of devices now connect to enterprise resources from inside and outside the perimeter of the enterprise, effectively reducing the perimeter to near zero. These developments are a source of both great advantage and great risk. Yet, many enterprises remain overly reliant on disparate siloed, poorly connected network infrastructure and cybersecurity tools to manage, protect, and secure their operations.

Organizations Are Blind To Application Relationships

Most IT and security organizations have poor or limited visibility into their enterprise's true interconnectedness—the relationships and dependencies between and among users, applications, networks, and infrastructure; as well as how and where these applications are being accessed and utilized. These blind spots adversely affect understanding of policy intent and consistency across environments; and whether applications exist that are not being protected or accessed as they should.

To fully grasp security and operational risk, enterprises must understand the totality of the relationships among users, applications, and workloads. Not seeing or understanding these relationships increases risk through security breaches, data theft and loss, application outages, and non-compliance—all with serious implications to the organization's brand reputation, revenue potential, customer satisfaction, and regulatory standing.

Most existing approaches to these challenges are vestiges of on-premise models and thinking. Most were not natively designed for modern deployment environments. Conventional approaches that attempt to stitch together uncorrelated data from network and infrastructure silos remain difficult to do and scale in modern, highly dynamic enterprises. Not surprising therefore that enterprise IT security still relies heavily on a perimeter-based protection methodology.

Enterprises compensate for this lack of real-time visibility by using abstraction processes and people with site knowledge to operate brute force methods that approximate their business. This is neither desirable nor sustainable. Organizations become hamstrung trying to cope with multifold increases in business complexity without commensurate increases in headcount, or adding more point solutions that provide only partial efficacy. This approach has alarming implications: decisions and actions are based

on a limited, snapshot view of the environment. This in turn affects deploying new capabilities, implementing cloud migration, determining security policy accuracy, assessing incident response, and regulatory compliance.

A New and Transformative Approach for Modern Environments

Nowadays, enterprises are paced by and reliant on the deployment and use of interconnected software applications, rather than networks, hardware, and infrastructure. Solutions to manage enterprise risk and security must embrace this reality. ARM lies at the intersection of applications and users—and the dynamic relationships and interactions between and among them. With ARM, organizations can visualize applications, application relationships and dependencies, and identities (such as users, devices, machines, and service accounts) in real-time across the entire enterprise.

ARM solutions let you create, enforce, and validate policies that apply application-centric security and operational controls based on what you see now. With ARM, enterprises can fully understand the totality of interactions or communication between applications, workloads, and identities. Because ARM does not require the deployment of new infrastructure, organizations leverage the investments they already have in place. Enterprises can address critical use cases that are impossible currently, or are otherwise difficult, inefficient, and costly. All without the disruptions caused by sizable new infrastructure investments or "lift and shift" demands.

What ARM Means for Enterprises

With ARM, enterprises gain unprecedented visibility and insights into all their applications across every environment. Real-time visibility yields more insights, more easily, than those gleaned from abstractions, sampling, or estimates. With greater operational understanding and confidence, organizations can make better, faster decisions that significantly improve business performance, resiliency, security, and customer satisfaction; and commensurate reductions in business and operational risk through adverse compliance or regulatory exposure. With ARM, enterprises can reduce enterprise-wide risk and demonstrate that they are doing so from observed reality to:

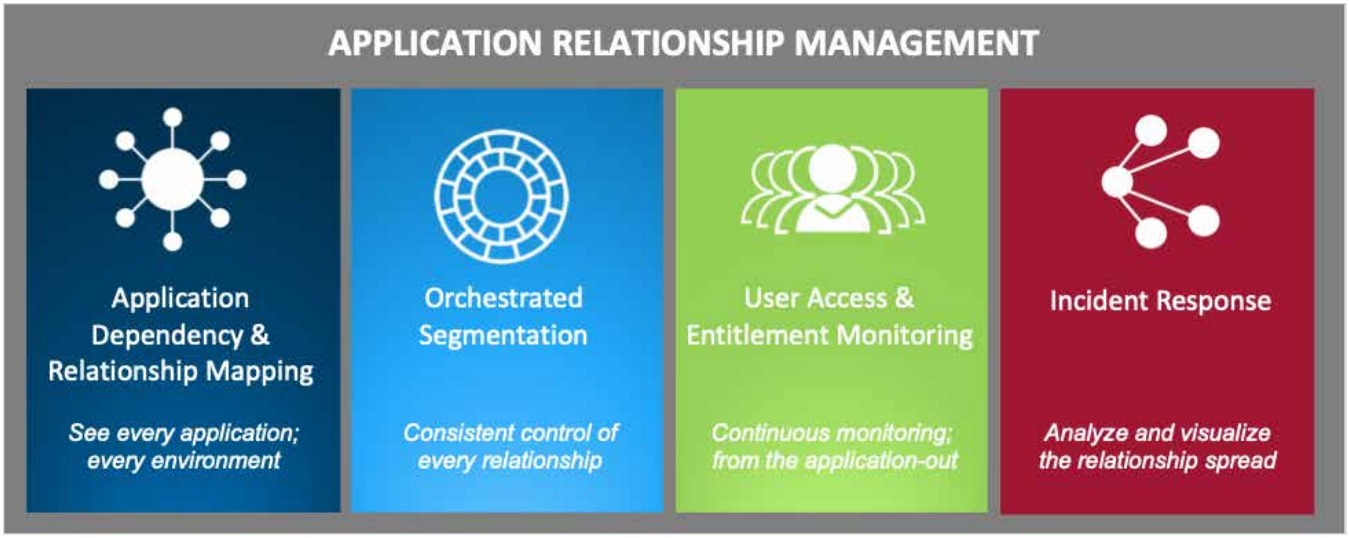
- Protect and secure business operations operating in zero perimeter environments.
- Facilitate and maintain digital transformation initiatives, even in heterogeneous environments for greater responsiveness, agility, and efficiency.
- Address regulatory requirements, enable more comprehensive governance frameworks, and demonstrate regulatory compliance.
- Simplify operations and reduce operating costs by relieving teams of people from tedious manual tasks with software that automates and scales consistent, accurate, and actionable intelligence for the business.

A Platform with Innovative Building Blocks

An ARM platform leverages several key technology differentiators to enable its unique solutions, including:

- An API-first approach that does not require agents or appliances, enabling platform-independent solutions for visibility and control.
- Modern Graph technology to efficiently ingest, compile and store massive amounts of application relationship data for visualization, analysis, and report generation.
- Ground-breaking, intuitive data visualization for easy comprehension.
- Relationship search functions for natural language or declarative queries that deliver easily understandable answers.
- A policy engine that uses advanced ML/AI for behavioral analysis, baselining and anomaly recognition based on application relationship behavior.

vArmour's ARM platform provides innovative software-based, software-defined modules to address major use cases: from visualization of application relationships to identities, to information flows, policy creation and enforcement, and incident response.



The Time Is Now

In the world of blurred or zero perimeters and accelerated digital transformation, businesses are more dependent than ever on connecting people within and outside the enterprise, and on applications that connect with other applications. These relationships matter. vArmour, the leader in Application Relationship Management, is devoted to helping businesses solve these challenges effectively, efficiently, and securely. See what you've been missing.

Application Relationship Management Solutions

Application Relationship Management comprises four broad solutions, all based fundamentally on enterprise-wide capabilities to visualize applications and their relationships between users, and between other applications, both in real-time and through historical views. These include:

1. Orchestrated segmentation
2. User access and entitlement monitoring
3. Application relationship and dependency mapping
4. Incident response and relationship search

 | 650.564.5100 | info@varmour.com | 270 3rd Street, Los Altos, CA 94022