Application Access & Identity Module Data Sheet

APPLICATIONS ARE THE NEW PERIMETER. DO YOU KNOW EVERYONE WHO'S ACCESSING THEM?

The vArmour Application Access & Identity Module enables enterprises to monitor and control who is accessing applications so that enterprises can continuously audit, respond, and control identities and access relationships.

As enterprises evolve and expand beyond their traditional perimeter—applications moving from the data center to the cloud, and employees moving out of the office to be more mobile and distributed—identity-based security has taken on a critically important role, especially for organizations adopting a Zero Trust security model. A mix of IGA, IAM, and PAM solutions have been adopted by enterprises to address this, but they only deal in the hypothetical. In other words, permissions are managed for what users *should* be able to access, but they don't tell you what *is* being accessed.

This static, often brittle set of policies results in a number of significant security challenges. First, the organization is blind to the relationships between applications and users, resulting in over-privilege and entitlement risks. Incident response efforts fail to meet time to contain objectives, lacking timely, critical synthesis of which applications, users, and systems are involved. Finally, securing the distributed workforce is difficult when access policies cannot be accurately observed, simulated and orchestrated across the enterprise's network and security infrastructure assets.

The Application Access & Identity Module, part of the vArmour Application Controller product, is the only solution that enables enterprises to visualize and control user relationships from the application-out.

Control Access Risk and Ensure Compliance

Efficiently identify and control areas of user access vulnerability and risk.

Accelerate Incident Response

Rapidly define and control the blast radius of an incident.

Validate Access of a Distributed Workforce

Create accurate privileges for an increasingly dispersed enterprise.

KEY BENEFITS

Visualize and Control User Access to Applications

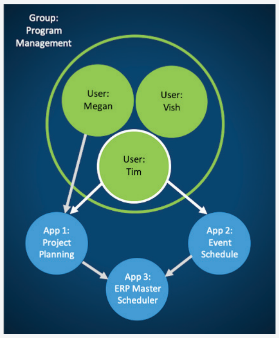
Protecting your most critical assets means first visualizing and understanding who has access to them, and then determining whether they should have access. vArmour enables customers to see identity from the application out. That is, extending vArmour's powerful ability to discover and understand applications across the enterprise to include what users and devices are accessing them so that risk can be managed.

Continuously Monitor Real World User Access Behaviors

Only vArmour takes your policy intent, and translates that into reality. Simply declare your intent—increase resiliency; reduce risk; or ensure compliance—and vArmour automatically computes both monitoring and enforcement policies. We'll even simulate the effects of policy changes before implementing so you can deploy with confidence. vArmour transforms manual, error-prone processes that took weeks or months into a simple click.

Expedite and Coordinate Changes at the Speed of Business

The process of updating security policy is rigid, struggling to adapt to economic disruptions and the evolving needs of the business. vArmour accurately simulates, predicts, and responds to the changes on your users and apps – who's impacted, and in what way?



USE CASES

Risk and Compliance

Continuous behavior monitoring of actual and attempted access from the application out—no hypotheticals.

- Identify which roles and groups are accessing your applications
- Determine if access matches up with your governance and compliance policies
- Automate your entitlement and de-entitlement process, decreasing or even eliminating the time and cost associated with application access audits

Incident Management

Expedite containment by visualizing the relationship map from user to app to app—what's impacted, and in what way.

- What are the relationships and blast radius?
- Identify which users, devices, and applications are involved, and when
- Clearly and quickly communicate the blast radius to stakeholders to drive remediation and notification decisions

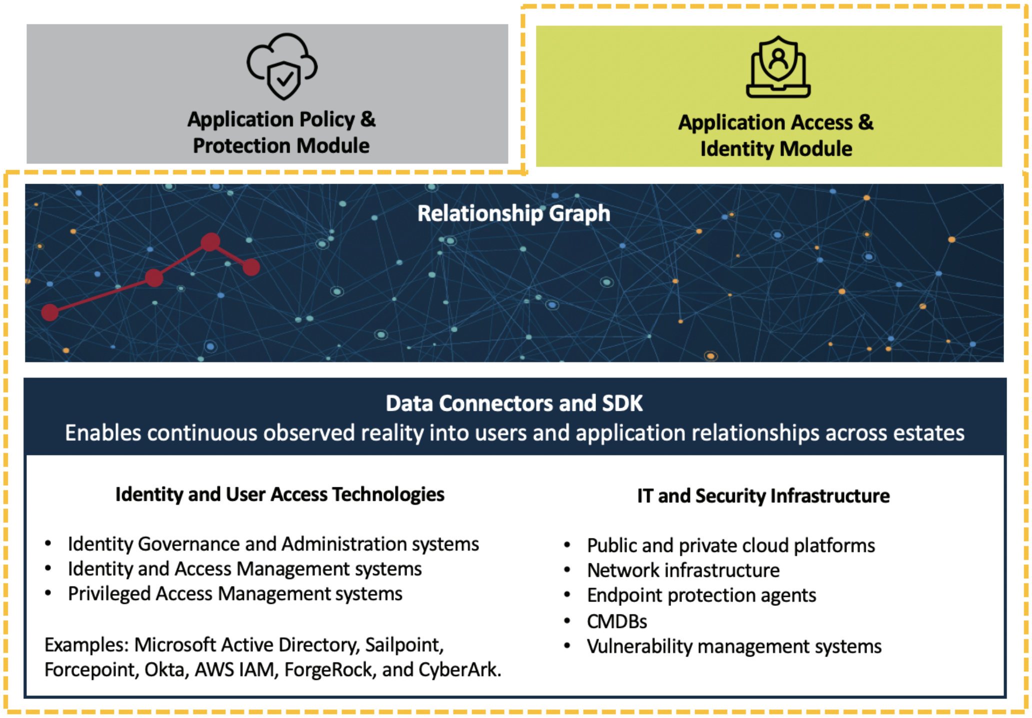
Distributed Workforce

Visualize and control access to any system over any protocol and port—every environment, every channel.

- Deliver Zero Trust relationship controls for a distributed workforce without disrupting the business
- Determine if your remote users are using appropriate access
- Assure that your security controls are effective

INTEGRATES WITH YOUR EXISTING IDENTITY AND USER ACCESS TECHNOLOGIES

The Application Access & Identity Module is part of vArmour Application Controller, a modular software solution for securing enterprise-wide relationships. Data connectors make it simple to integrate the existing identity management technologies you already have deployed at your organization. The Relationship Graph uses telemetry from these systems to build a map of users and application relationships within and across your heterogeneous environments, enabling you to visualize and control real-world user behaviors and risks.



Application Policy & Protection Module

Application Access & Identity Module

Relationship Graph

Data Connectors and SDK

Enables continuous observed reality into users and application relationships across estates

Identity and User Access Technologies

- Identity Governance and Administration systems
- Identity and Access Management systems
- Privileged Access Management systems

Examples: Microsoft Active Directory, Sailpoint, Forcepoint, Okta, AWS IAM, ForgeRock, and CyberArk.

IT and Security Infrastructure

- Public and private cloud platforms
- Network infrastructure
- Endpoint protection agents
- CMDBs
- Vulnerability management systems

vArmour Application Controller shown with Application Access & Identity Module