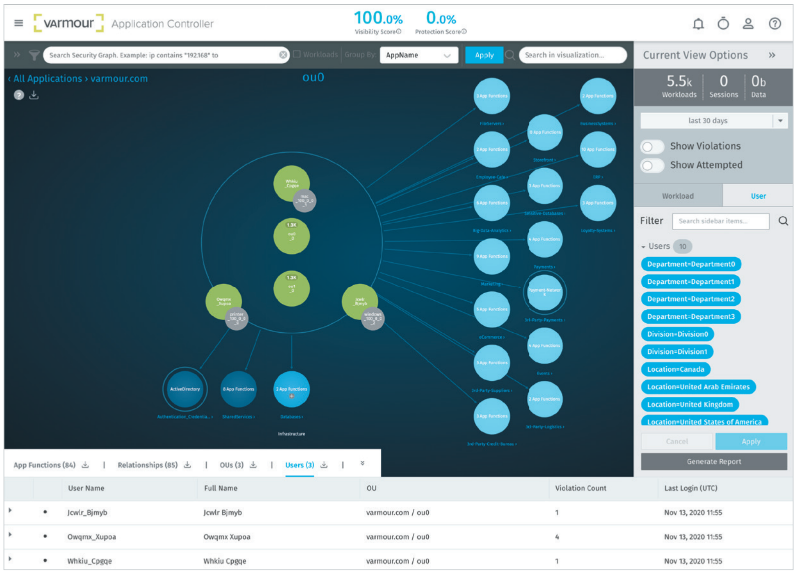
USER ACCESS & ENTITLEMENT MONITORING
SOLUTION BRIEF

Business Challenge: Managing Entitlement and User Access to Enterprise Apps

As business goes digital, employees need access to apps no matter where they are located. Even before the pandemic, many organizations had become reliant on a highly distributed workforce using many different devices across many different networks.

In a dynamic business environment, both apps and users can change frequently, increasing the risk of entitlement drift, unsanctioned app access, compliance issues and security risks. Without robust controls, enterprise software can be accessed by malicious or unauthorized users, either directly or through backdoors from related apps: the organization is left exposed and vulnerable.

Using fragmented legacy identity systems to control access to apps hosted in multiple clouds can be a struggle. As these tools aren't able to provide a unified view or insights, organizations are faced with the time-consuming and expensive task of manually stitching together a comprehensive picture of entitlements and user access.



		User Name	Full Name	OU	Violation Count	Last Login (UTC)
▸	•	Jcwlr_Bjmyb	Jcwlr Bjmyb	varmour.com / ou0	1	Nov 13, 2020 11:55
▸	•	Owqmx_Xupoa	Owqmx Xupoa	varmour.com / ou0	4	Nov 13, 2020 11:55
▸	•	Whkiu_Cpgqe	Whkiu Cpgqe	varmour.com / ou0	1	Nov 13, 2020 11:55

Figure 1. Visualize, identify and control user entitlements and privilege gaps that increase risk.

Why vArmour?

App-centric view of what is actually happening

Unlike other solutions, vArmour provides an app-centric, multi-dimensional view of who is actually accessing an app, as opposed to a hypothetical view based on the preconfigured permissions. It also shows failed attempts to access an app, potentially alerting the organization to malicious activity.

Combining identity and app interdependencies

vArmour was the first vendor to provide a unified view by integrating identity management with the relationships between apps. That provides organizations with a high level of visibility and control over user access to apps.

Comprehensive and dynamic

To complement existing identity access solutions, vArmour can display user and app relationships in a single enterprise-wide view, while dynamically tracking who is accessing which apps. The solution automatically discovers users and apps, and computes app-centric monitoring and enforcement policies.

Straightforward attestation

vArmour's Application Access and Identity Module simplifies access attestation and entitlement management by providing an app-centric view of access and entitlements.

Product and Module

Application Controller
Application Access & Identity Module
Application Policy & Protection Module

vArmour's User Access & Entitlement Monitoring Solution

To help organizations curb unsanctioned or malicious usage of apps, vArmour's Application Controller includes a module that can visualize, validate and control user access and entitlements across an entire IT estate. Taking an app-centric view that cuts across organizational silos and heterogeneous multi-cloud environments, the vArmour solution can display end-to-end user access information in near real-time. It can also validate and consistently enforce entitlements, thereby reducing the number of over-privileged and unauthorized users. As a result, the organization will lower its operational risk and costs.

Straightforward to deploy rapidly and scale, vArmour's fully customizable solution provides a multi-dimensional view, encompassing both historical app relationships, as well as the current and potential state of play. Equipped with comprehensive filters and search capabilities, it can enable security teams to understand complex user access and app relationships, identifying potentially toxic combinations that could lead to security risks and compliance violations. Customized compliance reports can be generated in hours, rather than months, leading to better governance and a consistent user access policy across all environments. In this way, vArmour can dramatically reduce the organization's security threat surface.

Key use cases

Continuous monitoring of access to apps

Unsanctioned app access can result in security risks and compliance or regulatory violations, particularly in a dynamic business environment where the organization doesn't have an up-to-date view of who is using which apps.

To greatly reduce such risks, vArmour's solution detects in near real-time any anomalies from baseline app behavior. It can also alert an IT organization to any discrepancies between its access policy and what is actually happening. By identifying issues before they become too big or impactful, the solution dramatically reduces the business risk from unsanctioned or malicious access to apps.

Managing access for remote workers

Inconsistent and unevenly applied access policies can lead to over-privileged app users and cloned privileged users, as well as entitlement and credential drift.

With vArmour's solution, an organization can apply flexible filters that can show which apps are being used by which users over which time periods. It can also be used to both highlight variances in, and violations of, user access policies and then refine the rules accordingly. The combination of better governance and compliance, near real-time validation of app usage and a reduction in the threat surface can substantially reduce operational risks for organizations.

Compliance validation and reporting

In a dynamic IT environment spanning multiple clouds, manual compliance processes are proving to be both time-consuming and ineffective.

Designed to automatically report on actual user access to apps, vArmour's solution delivers detailed, accurate and comprehensive auditing and attestation to meet compliance requirements. As a result, it streamlines compliance for app access from months to hours, enabling the business to focus on more productive tasks. That translates into lower costs to comply with regulatory mandates, such as FFIEC, GDPR, and SWIFT CSP.

Entitlement monitoring and enforcement

Entitlement drift can give rise to both operational and security risks by opening the door to abuse of access privileges by employees, partners and third party contractors. It can also increase the organization's software licensing fees, as it may be paying for seats it doesn't need.

By enabling an organization to easily visualize, identify, and control user access to each app, vArmour's solution can reduce the risks and costs associated with entitlement drift. Unnecessary entitlements, over-privileged users, and unauthorized users quickly become apparent, enabling the IT organization to streamline access rights. The solution can also be used to highlight and eliminate unused access rights, thereby lowering software licensing costs.