VARMOUR AND OKERA ENABLE SECURE IDENTITY-BASED ACCESS TO APPLICATIONS AND DATA ACROSS HYBRID ENVIRONMENTS

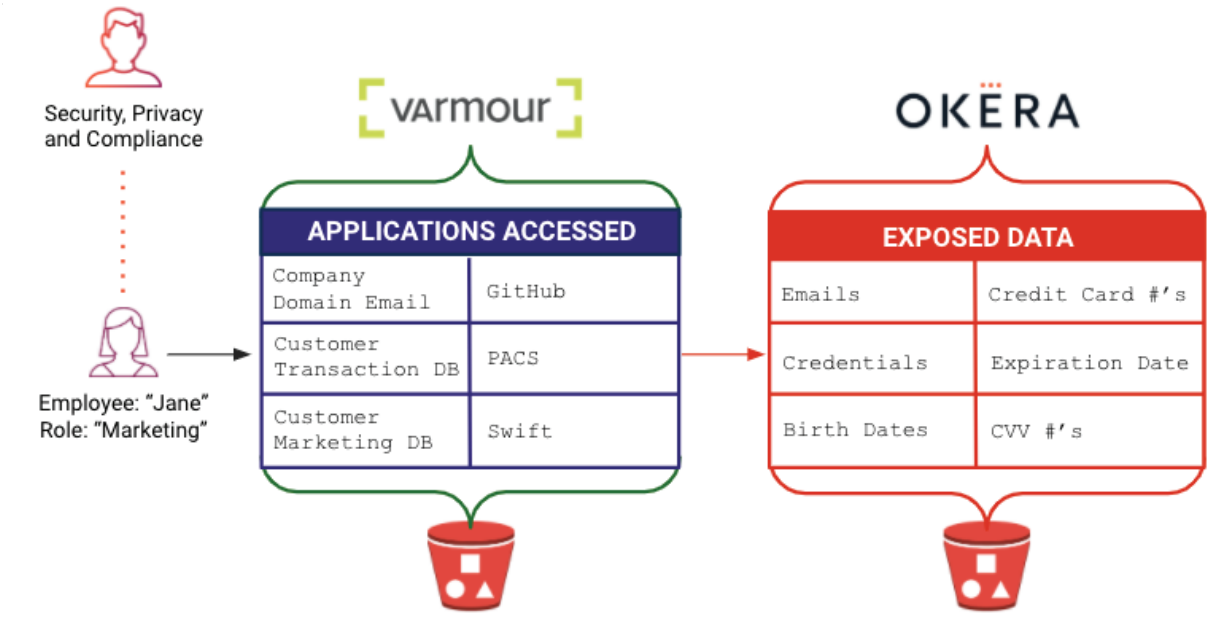
The Challenge: Organizations Face Complexity and Risk in Application Infrastructure.

Enterprises are currently struggling to navigate a perfect storm within their IT infrastructures, which has the potential to compromise their security posture, exacerbate business risk, and disrupt their regulatory compliance. This storm is the result of a confluence of major events: the growth in and strategic importance of applications to enterprises with digital transformation, the rapid shift in hosting application from private data centers to public clouds, and the immediate impact of COVID-19 to a newly remote workforce spread around the globe.

According to the 2019 Verizon Data Breach Investigations Report, 80 percent of security breaches resulted from compromised or weak access credentials. Furthermore, a breach lifecycle under 200 days costs $1.2 million less than a cycle over 200 days, according to IBM Research. Meanwhile, the impact of those breaches is not fully measurable because complex application relationships often exist that create hidden pathways among unauthorized users and data systems. This makes it difficult to quickly mitigate security incidents by identifying source users, devices and required steps to contain breaches. What is a CISO to do?

Unfortunately, what exists today are a patchwork of tool and analytic siloes that provide limited views of applications, environments and data, significantly increasing the complexity for security operations and infosec teams, providing partial visibility that may still fail to protect enterprises from material security threats and business risks.

Enterprises urgently need a comprehensive solution that visualizes the entire application infrastructure, identifies unknown relationships and underlying data, while simplifying the ability to secure user access to all applications and related data.



vArmour and Okera secure user access to critical data by providing a user-centric view of application relationships and related data

vArmour provides visibility and control for all applications in an organization's IT infrastructure across public and private cloud environments, like a "Google Earth for the Enterprise." Similarly, Okera provides visibility and control for all the applications' underlying data, often the crown jewels that attackers aim to exfiltrate. Together, the unified solution from vArmour and Okera enables customers to gain a comprehensive user-centric view of the applications and related data.

vArmour's powerful software quickly and intuitively uncovers the unknown relationships, dependencies, and vulnerabilities that may cause security threats and business risk. In addition, vArmour can now incorporate enterprise user data and access control policies based on user access credentials, devices, location, and applications for even more insight into security and compliance.

As part of the joint solution, Okera extends the fine-grained visibility and control you gain from vArmour to the critical underlying application data, such as usernames and passwords, credit card numbers, and Social Security numbers, birthdates and other sensitive, personally identifiable information (PII) and protected health information (PHI) that absolutely cannot be compromised. Okera automatically defines, enforces, and audits data access policies using an intuitive zero-code interface, enabling secure data access and governance at scale. In addition, vArmour can now represent Okera's insights on sensitive application data within its easy-to-use application relationship management interface. As a result, organizations can quickly gain a comprehensive understanding of their risk posture across applications and data like never before.

With this partnership, vArmour and Okera enable organizations to:

- Simplify security operations and reduce time to resolve with a comprehensive solution that visualizes enterprise application relationships and related critical data
- Reduce business risk by understanding and enforcing how and when distributed workforce users can access applications across hybrid environments
- Meet and sustain regulatory compliance requirements via data privacy protections, auditing, and reporting capabilities
- Mitigate attack vectors and suspicious user access to applications by surfacing hidden dependencies and unknown access privileges across the application portfolio

USE CASES

Fully Visualize Application, User, and Data Relationships: Find out the full extent of the relationships among applications and data, how and when users access both, and how that relates to existing application access and data security policies, who is accessing what sensitive data and when. Determine the type of data an application has access, and if the data is sensitive, provide a data first approach to security.

Audit and Compliance Automation: Shift from time-consuming manual processes to automated documentation compliance reporting and enforcement of requirements that govern application access.

Identify Toxic Combinations: Visualize and control toxic application access combinations for improved governance and compliance, such as over privileged users accessing sensitive data and unauthorized users accessing (e.g. Trading users accessing research applications; Non-privileged users accessing privileged systems.)

Data First Approach to Security Assurance: Drill down to see beyond fine-grained per-user access to applications and their connections right into specific, sensitive application data attributes to ensure regulatory compliance.

Identify Suspicious or Malicious Actors: Uncover and flag questionable and unsanctioned access to applications and data by unauthorized users. Flag unusual access patterns based on location or device type. Reduce attack vectors and business risk application access by accounts (whether stolen or by incorrect usage) or patterns (e.g. location) that access new or out-of-policy systems.