Hiding in Plain Sight

How a Cloud Access Security Broker with Built-In User Behavior Analytics Unmasks Insider Threats in the Cloud

ORACLE WHITE PAPER | JANUARY 2017

Introduction

Chief information security officers (CISOs) are concerned with data confidentiality, integrity, and availability—also known as the CIA triad. This triad is a model designed to guide policies for information security within an organization. In theory, maintaining compliance should alleviate the concern with data CIA. However, the sprawl of software as a service (SaaS), rapid adoption of infrastructure as a service (IaaS), erosion of the network perimeter caused by bring-your-own-device (BYOD) policies, and explosion of unsanctioned cloud applications amplify security issues CISOs face.

With these new threats brought on by cloud pervasiveness and BYOD, many CISOs focus on external threats and overlook the most active threat to their cloud environment—the insider. The statistics vary, but industry experts consistently state that a majority of threats come from insiders: employees, contractors, consultants, and unprovisioned ex-employees.

Many of the controls put in place to mitigate cloud security threats fail to protect the enterprise against a user with valid credentials. This white paper examines how cloud access security brokers (CASBs) with user behavior analytics (UBA) can combat insider threats.

Traditional Authentication Methods Fall Short

In addition to industry or business-specific functions, the responsibility of a CISO encompasses:

- Physical and logical access controls
- Perimeter management via security appliances such as virtual private networks (VPNs), firewalls, and proxies
- Data classification, tagging, and encryption
- Security operations and incident response
- Governance and compliance monitoring and audit support
- Education programs

Controlling these fundamental areas of information security relies on a single premise: *your user is who he says he is.*

Traditional authentication methods, the foundation of identity management, don’t increase your assurance against a set of compromised credentials. Educating users about security best practices is only mildly successful. CISOs need to arm themselves with a richer set of information. They know whose credentials are used to gain access to business-critical assets, virtual infrastructure, and data—but they do not know which user is using those credentials. That is not enough.

> *Malicious and unintentional insider threats are pervasive and difficult to thwart. In fact, 74 percent of organizations surveyed feel vulnerable to insider attacks, but only 42 percent feel that they have the controls in place to prevent internal assaults.*
>
> **2016 INSIDER THREAT SPOTLIGHT REPORT**

Update Your Security Approach to Assume Insiders Are a Threat

Balancing data protection and data accessibility relies on a deep understanding of your users and how they interact with your services. The traditional approach to security focuses more on the perimeter and the data than the user. This data-centric approach to security scrutinizes technology and processes to ensure that the data—your gold mine—is secure.

Data-centric security relies heavily on authentication as a key control. While these controls are necessary, they are insufficient against an insider threat. If someone already has legitimate credentials, many identity management controls will not prevent that user from taking action, whether malicious or benign. A CASB with built-in UBA turns this view sideways and adds a user-centric approach to security, allowing CISOs to secure both the gold mine and the miners.

Trust, but Verify the Actions of Your Employees

Classifying, tagging, and encrypting your data may help you secure data at rest and in use, but it won't protect your organization against the actions of users who already have authorization to use that data. A CASB with built-in UBA complements security solutions and security measures built into cloud services. With intelligent analysis of user behavior, UBA can detect suspicious activities, malicious activities, and even identify risky user behavior before a breach occurs.

Monitoring user behavior plays a critical role in your organization's information security strategy, providing CISOs the ability to engage in the "trust, but verify" model. UBA increases the ability of security operations to view threats from the user, separating the use of account credentials from the actor using the account credentials. User behavior focuses on the actor and the transactions that he executes, which provides context beyond mere credentials. There is no way to detect a compromised account from your data manually. Yet this additional analytical context can surface patterns of abnormal behavior and act as a fourth factor of authentication: something you know, something you have, something you are, and the pattern of things you do.

Humans reading log files and manually reviewing application transaction logs cannot enforce these controls. Identifying abnormal usage from transactional logs in a timely manner and then acting upon that information can only be accomplished using machine learning and heuristic reviews of these massive data sets. UBA simplifies the process of securing your assets by analyzing users' usage patterns automatically and provides continuous threat intelligence to enable security operations to act on the information in a timely manner.

How a CASB with Built-In User Behavior Analytics Enhances Security

A CASB with machine learning monitors user behavior and looks for abnormal usage patterns of cloud applications. The CASB sets a baseline of standard behavior for each user by monitoring all user and service account activity. With this baseline of normal behavior, your security operations team can detect anomalous usage to address an insider threat. User behavior analytics within a CASB continuously compare user behavior against the baseline to detect anomalous activity. Abnormal usage may indicate a malicious insider, a compromised account, or completely innocuous user behavior.

In addition to comparing a user's behavior to his historical baseline, advanced UBA models incorporate peer data, comparing the user to similar employees to determine if usage patterns are abnormal. Functional models indicate which users warrant further investigation to security operations.

A CASB with built-in UBA is a powerful tool for identifying compromised accounts and insider threats. Machine learning with heuristic analyses is the only way to uncover this information from the massive quantities of data your applications produce.

Real-World Examples: CASB with Built-In User Behavior Analytics in Action

Here are two real-world examples in which a CASB with built-in UBA detected an insider threat in the cloud.

Example #1: Bitcoin Mining

An employee in a company with the majority of their operations in the US, decided to leverage the organization's AWS environment for the purpose of Bitcoin mining. Knowing that the organization operates primarily within the US, the employee turned on Amazon Elastic Compute Cloud (Amazon EC2) instances in Asia at the end of each business day and then turned them off before the office opened each morning. No one had any reason to check if Amazon Web Resources (AWS) resources were being used outside the US, and hence, no one knew what was happening until a CASB with built-in UBA was brought in.

The company deployed Oracle CASB Cloud Service[1] to monitor user activity and behavior. It ingested the Amazon Simple Storage Service (Amazon S3) bucket logs and CloudTrail service logs—enabled for all regions and stored on a central Amazon S3 instance. Using machine learning and heuristic analyses, the UBA engine in Oracle CASB Cloud Service profiled all of the users and service accounts accessing the company's AWS account. It also tracked identity and access management (IAM), Amazon EC2, VPN, virtual private cloud (VPC), security group, and network access control list (ACL) transactions from the users' home and work laptops to establish normal behavior for each user and service account.

Using individual profiling, the company quickly discovered that one of its administrators was using the company's AWS instances to mine Bitcoins. As an admin, this user was trusted to configure and maintain the business-critical infrastructure and assets—yet he perpetrated a theft. The financial impact resulting from additional AWS instances was significant. In addition to the cost of the AWS instances, there was a risk of potential legal impact since some Asian countries ban Bitcoin. The CISO and CIO took action to engage legal counsel and terminate the employee.

Example #2: Theft of Customer Data

Salesforce provides a cloud-based solution for all aspects of sales and customer relationship management, enabling companies to utilize functionality quickly without requiring information technology resources to deploy.

One company decided to use Salesforce to manage its sales and account management processes. Each week, the VP of sales reviewed high-value and high-probability targets with the sales team to drive targeted campaigns in an effort to close outstanding deals.

The company deployed Oracle CASB Cloud Service with built-in UBA to monitor Salesforce activity and ensure that users and administrators were not compromising business-critical data. The CASB solution quickly built a profile for each member of the sales team, which included the third-party applications that each user added from the Salesforce marketplace.

An employee in the sales department gave notice so that he could pursue employment with a competitor. The employee then logged into Salesforce and made mass changes to customer account values. He downloaded a custom report to capture the recently-changed customer data with the intention of following up with these prospects in his next role. When the IT team investigated the alerts of anomalous activity, they found that the values of several

[1] Oracle acquired Palerra in September 2016. The customer used Palerra's LORIC product, now called Oracle CASB Cloud Service.

high-value prospects had dropped to $0. Because they were $0, these prospects were no longer visible on the report that the VP of sales reviewed weekly with the sales team. It was a perfect plot that would have gone unnoticed without Oracle CASB Cloud Service. As soon as the employee made mass changes to customer data, the CASB flagged the anomalous activity. Armed with this information, the company was able to take action.

Addressing the Insider Threat

Ensuring data confidentiality, integrity, and availability are critical responsibilities of any CISO. Yet the rapid adoption of SaaS and IaaS, erosion of the network perimeter caused by BYOD, and the explosion of unsanctioned applications significantly amplify security risks. Most CISOs focus on external threats when, in reality, the majority of issues in the cloud come from insiders.

It is impossible to hire enough security resources to sort through the mountains of data on user behavior to identify and remediate insider threats. There is simply too much data to monitor, process, and remediate manually. However, the consequences of a breach are significant including financial loss, tarnished brand reputation, or even loss of a job. To address insider threats affecting the modern cloud footprint, a CISO must implement a CASB that includes advanced UBA to automatically detect and prioritize internal threats, enabling organizations to realize the full benefits of the cloud.

Learn More about Oracle CASB Cloud Service

Oracle CASB Cloud Service is a leading cloud access security broker (CASB) with an innovative approach to securing your entire cloud footprint. As the pioneer of API-based CASBs, Oracle CASB Cloud Service is the only solution that provides visibility and security across software-as-a-service (SaaS), infrastructure- as-a-service (IaaS), and platform-as-a-service (PaaS) environments.

ORACLE®

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

- blogs.oracle.com/oracle
- facebook.com/oracle
- twitter.com/oracle
- oracle.com

Integrated Cloud Applications & Platform Services

Hiding in Plain Sight: How a CASB with Built-In User Behavior Analytics Unmasks Insider Threats in the Cloud
January 2017