OBSIDIAN

DATA SHEET

Account Compromise

Detect and mitigate SaaS account compromise in its earliest stages.

Overview

The volume of sensitive data entrusted to SaaS applications in recent years has created an inflection point in information security. Malicious actors are targeting SaaS with greater frequency and sophistication, bypassing traditional measures such as single sign-on and multi-factor authentication using methods like token compromise or supply chain compromise. After initial access, adversaries are hard to detect, and the interconnected nature of SaaS means that entry into one business-critical application can likely enable them to move laterally into a multitude of others. Security leaders recognize that existing solutions don't look within and across applications, creating a gap when it comes to detecting and mitigating SaaS compromise.

The Security Challenge

Better protection against account compromise begins with a complete picture of all users, permissions, and activity across your business-critical applications—but achieving this deep, consolidated understanding is no easy task. The services your business relies on are inherently complex, their data models can be difficult to retrieve, and user identities are typically fragmented across multiple accounts. After collecting this foundational context from your SaaS environment, your security team then needs to develop models that can detect intrusions across various applications and stages of account compromise with high fidelity.

Existing solutions don't solve these challenges or identify SaaS account compromise. Identity and Access Management (IAM) can be bypassed and decouples authorization from authentication, enabling attackers to make changes within applications. Cloud Access Security Broker (CASB) focuses on traffic inspection, applying binary rules to enforce data loss prevention and restrict use of unsanctioned applications. Security Information and Event Management (SIEM) can be configured with specific rulesets to detect client and infrastructure anomalies for individual users from log files, but as they don't understand the applications themselves, they're unable to detect unusual behavior inside the SaaS platforms.

Obsidian detects a variety of SaaS account compromise approches across our customer base, including:

Use Case

SSO Token Compromise

Attacker Steps: Use malware or a combined phishing and MITM attack to capture the SSO session token granted to an authorized user after a successful authentication. The attacker then reuses the same token as the user to log into the SSO platform directly, bypassing authentication controls like MFA and accessing any connected application.

Detection: Obsidian profiles each user's application session over time and identifies anomalous sessions which appear to have attributes of both the authorized user and the attacker using the same token.

Use Case

Cross-App Compromise

Attacker Steps: Gain initial access to a business-critical SaaS application using valid credentials, brute force, or other methods. Persistence can be obtained by modifying MFA settings or creating a mailbox forwarding rule. The attacker moves laterally across integrated applications.

Detection: Obsidian identifies cases of impossible travel by examining geolocation data from authentication and post-authentication events within and across applications. Our model contrasts this data against historical trends for the user and organization to flag an attacker's initial access.

Mitigate Account Compromise with Obsidian

Building a foundational knowledge graph

The ability to identify account compromise with a high degree of accuracy requires a comprehensive understanding of users and their activity across applications. Obsidian applies a deep understanding of each service to map complex data schemas across SaaS applications using inputs from hundreds of APIs and various protocols. We seamlessly connect to your business critical applications within minutes and immediately begin to:

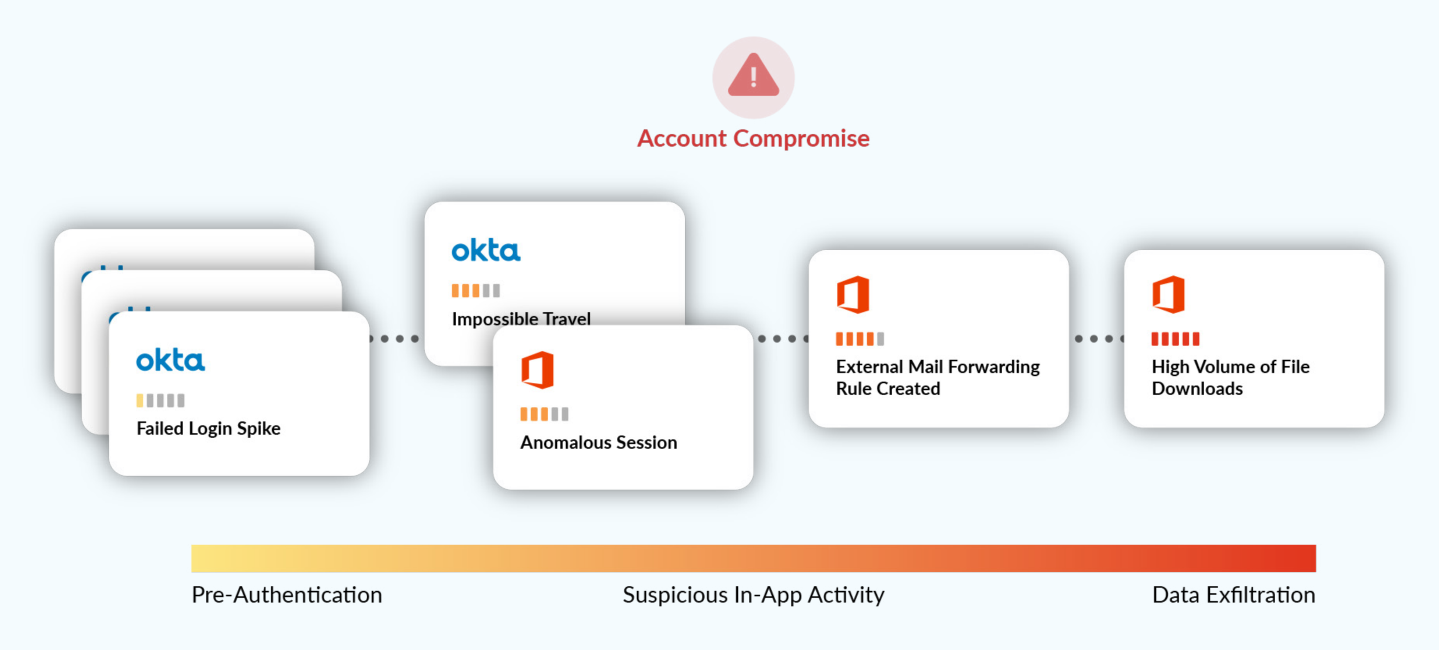
- ✓ Retrieve users, activity, privileges, and configurations
- ✓ Deduplicate and normalize events to our Obsidian format
- ✓ Enrich events with context, such as threat intelligence and geolocation
- ✓ Resolve multiple accounts across applications to a single user entity

The result is a proprietary knowledge graph with one standardized data model that serves as a platform for threat detection and provides a comprehensive view of each user and application.

Interpreting user activity

Obsidian security researchers and detection engineers work collaboratively on detection models for account compromise. Our models look both deep within SaaS applications for service-specific threats, as well as across your business-critical applications. These models are continually refined using confirmed account compromises from Obsidian's diverse customer base, resulting in a more accurate model than any one environment can provide. We also analyze the latest tools and techniques employed by malicious actors to develop state of the art detections. Security teams with more specific concerns can easily complement Obsidian's rich compromise models by creating their own detections to continuously monitor for custom-defined behavior patterns.

Obsidian leverages your historical data to circumvent the conventional tuning period, allowing us to deliver high-fidelity results immediately. We empower security teams with fast, efficient triage by supporting each compromise detection with actionable remediation recommendations and relevant contextual activity data looking back over a 90 day period.



Obsidian detects anomalous activity across applications at every stage of SaaS account compromise.

Identifying account compromise early in the kill chain

Obsidian identifies anomalous activity across stages of account compromise, combining multiple low-fidelity signals to catch sophisticated breaches that could otherwise be overlooked as noise. Our detections go beyond alerts, revealing important contextual information around a compromised user in order to quickly ascertain the exact impact of an attack. This context includes a breakdown of user privileges within various business-critical applications, a list of sensitive files accessed, and a detailed timeline of actions taken by the individual. We couple this information with recommended remediation actions, enabling security teams to act before persistence is established and data is exfiltrated.

Get started with a live demo

https://www.obsidiansecurity.com/demo/