VEROSINT

FAQs

Verosint: Smarter, Faster Detection & Prevention of User Account Attacks

Verosint stops cybercriminals from taking control of user accounts and attacking your business by using AI-powered behavioral analytics and identity intelligence signals to provide instant notification and detection of account takeover, credential stuffing, account sharing, fake accounts, and other account-based attacks. Verosint provides:

- Account attack and fraud dashboards
- Behavioral, threat and account analytics
- Device fingerprinting
- Credential intelligence
- Powerful OSINT signaling

Identity management systems and security event logs were never designed to provide this combination of deep visibility and behavioral analytics necessary to detect today's advanced attacks among thousands or millions of users, and 10's or 100's of millions of events generated every day.

This document will provide answers to common questions for organizations interested in evaluating Verosint and comparing it to other approaches to user account security.

Frequently Asked Questions

Q1: I thought my Identity and Access Management (IAM) platform provided adequate user account security. Why would I want to add something else?

IAM platforms are built to excel at provisioning users and granting them access to resources by verifying identity, often through a username/password combination, MFA token, or passkey. Their main focus is on determining the legitimacy of a user at the point of login—granting or denying access based on whether the credentials match. While many IAM systems now include basic risk scoring or attribute evaluations (e.g., impossible travel, new location), these are often limited in scope.

Verosint, on the other hand, goes beyond surface-level attributes, looking at user data more holistically. We focus on evaluating how users interact with each other and analyzing behavioral trends over time, allowing us to identify both individual and interconnected anomalies across your platform. This capability enables Verosint to flag not just risky events or behaviors on an individual basis but also detect larger patterns of anomalous activity across the entire application or enterprise. In short, Verosint provides deeper insights into user behavior and connection patterns, which traditional IAM platforms often overlook. These deeper insights are essential to detect and prevent attack from cybercriminals that have become increasingly sophisticated.

Q2: What type of data does Verosint collect? Can you provide some examples?

Verosint gathers Identity Action events from your IAM platform, application, or SIEM tool to analyze user behavior and connections. Typical event types include LOGIN_SUCCESS, LOGIN_FAILURE, PASSWORD_RESET, and others. (A complete list is available here: docs.verosint.com/page/event-types. **NOTE:** We continuously expand the list of supported event types.)

For us to evaluate user connections and flag unusual signals, we only need a few details from each event. Each event sent to Verosint requires: Email Address, Account ID, IP Address, and Event Type. For example, an event might look like this:

mark@example.com, mark, 9.9.9.9, LOGIN_SUCCESS

This entry tells us that mark@example.com (Account ID: mark) successfully logged in from IP address 9.9.9.9.

Q3: Is a direct integration with my IAM platform or application necessary to benefit from Verosint?

Ideally, a real-time connection provides the highest level of attack and fraud detection. However, we understand this might not always be immediately feasible, and some users may prefer to screen data historically or on a scheduled basis. If your data is stored elsewhere, you can still use Verosint's CLI tool or write directly to our API in batch mode according to your preferred schedule. Real-time integration is optimal but not required—we support multiple methods to suit different needs.

Q4: Is my data shared?

By default, all data within your Verosint tenant is exclusive to you and does not contribute to the Verosint Fraud Network unless explicitly opted in.

Q5: I have Okta Customer Identity Cloud (formerly Auth0). What permissions are required to enable Verosint?

For Okta CIC, Verosint offers two integration options available on the Okta Marketplace:

1. **Log Streaming Integration:** This integration provides intelligence-only insights and is simple to set up (approximately five clicks). It activates Verosint's insights and attack notifications. Enabling this requires an Okta Auth0 administrator with permissions to add log streams.
2. **Fraud Detection Integration:** This option allows for orchestration of user journeys at sign-in or sign-up based on workflows created in your Verosint tenant. It's also available through the Marketplace and requires administrative access to run as an action within your CIC tenant.

Q6: I use Okta Workforce Identity Cloud. What permissions do I need to turn on Verosint?

For Okta WIC, Verosint is set up as an Inline Event Hook. Documentation for configuration can be found here: docs.verosint.com/docs/okta-wic-log-streaming. Setup requires administrative access to your Okta WIC tenant.

Q7: I have PingFederate on-premises. How can I enable Verosint?

Events can be streamed directly from PingFederate to Verosint via policy. For documentation, please contact a Verosint representative.

Q8: I use PingDaVinci with PingOne Cloud. What is required to enable Verosint?

For PingDaVinci, documentation is available to guide integration. Verosint can be added to a DaVinci flow during sign-up, sign-in, or any event within a user journey. A simple API callback to Verosint supports event streaming, while an additional API call enables Verosint to participate in journey orchestration, enhancing visibility and signaling within Ping workflows.

Q9: I have ForgeRock (now Ping). How can I enable Verosint?

For ForgeRock on-premises, contact Verosint for further assistance. We have several implementation partners with built integrations for ForgeRock environments.

Q10: My application does not use an off-the-shelf IAM platform. How can I enable Verosint?

For custom applications, Verosint offers two straightforward API endpoints. The first endpoint receives event data from your application, and the second enables workflow orchestration to support advanced signaling and user journey management. This lets you integrate Verosint's signaling capabilities into your application without relying on an existing IAM platform.

You can signup for a free account from Verosint and directly experience Verosint's comprehensive user account attack discovery, notification and prevention solution for your organization.

Prefer To See A Demo Instead? In less than 30 minutes, we'll show you how to connect your data and start detecting and preventing account fraud and attacks. Contact us to schedule your demo.

VEROSINT

verosint.com/free

verosint.com/demo