

Imprivata Knowledge Hub:

Anomaly Detection

What is Anomaly Detection? Learn about this term and more with our expansive website glossary that explores topics related to enterprise access management.

Video Transcript:

Kayleigh Flemming: Hi, I'm Kayleigh with Imprivata!

Anomaly detection is a cybersecurity technique that identifies unusual patterns in user activity, network behavior, or system access that could indicate potential security threats. Analyzing deviations from established usage patterns allows organizations to detect and respond to unusual access patterns that may signal a security breach.

Anomaly detection is particularly valuable in privileged access monitoring. Privileged access refers to the elevated permissions granted to certain users, such as administrators, who have the ability to make significant changes to systems and data. These users are often targeted by cybercriminals due to the high level of access they possess. Anomaly detection helps distinguish between legitimate and suspicious activity, so that unauthorized actions are identified and addressed.

The process of anomaly detection involves several key steps. First, a baseline of normal behavior is established through the collection and analysis of historical data. This baseline serves as a reference point for what is considered "normal" activity. Once the baseline is established, the system continuously monitors user and network behavior in real-time. Any deviations from the established norms are flagged as potential anomalies. These anomalies are then analyzed to determine whether they represent a genuine security threat or a benign deviation.

Organizations that deploy anomaly detection systems benefit in numerous ways. One of the most significant advantages is the early identification of threats. By detecting unusual patterns early, organizations can take proactive measures to mitigate potential risks before they escalate into full-blown security incidents. Early detection also means that security teams can quickly investigate and respond to potential threats. This rapid response can significantly reduce the impact of a security breach, minimizing data loss and downtime.

At Imprivata, we deliver simple, secure access for critical workers and third-parties through features like Anomaly Detection.

[Contact us](#) to learn more.

Thanks for watching!

This information is intended to be for educational and marketing purposes only. Imprivata, Inc. delivers simple and secure access to all applications from any device and for all users, helping organizations increase workflow efficiency, improve cybersecurity, and drive return on technology investments.

© [Imprivata, Inc.](#)