Unauthorized Access Detection
Monitor and Mitigate Fraudulent Logins

Cybercriminals are using a wide variety of fraudulent methods to steal usernames and passwords and take over accounts. Credentials and some legacy user verification methods are no longer enough to keep fraud at bay, even successful logins confirmed by second authentication factors need to be thoroughly evaluated for evidence of suspicious behavior. Systematically monitor all user login activity to block irregular access attempts and launch next-generation push authentication that turns mobile devices into trusted authentication factors.

Highlights:

> Identify and stop unauthorized access to online portals to prevent compromise and fraud

> Instant alerts and full reporting about all suspicious logins

> Get visibility into when and where employees and customers are accessing sensitive data and accounts

> Comply with local and international regulations mandating login anomaly detection

> Authenticate logins with push notifications sent promptly to user mobile devices

> A wide variety of authentication methods, including innovative soft tokens and QR codes
Unauthorized Access Detection Features

Prevent Fraudulent Account Access with Complete Login Monitoring
Login anomaly detection is crucial for blocking unauthorized parties from gaining entry to your customer and employee accounts. Cyxtera’s Total Fraud Protection platform transparently safeguards your entire user population with no change to their online experience or extra software required, providing an extra layer of protection to systems that employ usernames and passwords to limit access.

Event Correlation and Immediate Alerts to Pinpoint Suspicious Login Activity
Cyxtera’s behavioral analytics are ideal for securing using accounts during login, because differences from normal user activity can still be detected no matter how credentials were stolen or what malware was used. Our analyzers are able to identify common patterns observed when unauthorized logins occur, including logins at unusual times and from new locations, trying credentials on several different systems, trying several sets of credentials on the same portal in succession, and many more.

Complete Reporting and Data about Login Statistics and Trends
Our detailed incident reports provide your organization with a wealth of information about how end users are interacting with your online portals. See which of your systems has the most login failures, find out which users who failed to log in across multiple systems, view login success rates and many more pieces of data that can help your organization create effective login incident response processes and procedures.

Assistance with Regulatory Compliance and Liability Protection
Oversight bodies around the world, such as the Payment Card Industry Security Standards Council, expect that financial institutions and other organizations handling sensitive information will implement solutions to prevent unauthorized access. Courts are also beginning to hold organizations liable for systems that fail to provide reasonable protection. Our unauthorized access detection platforms can give your organization the tools to meet security regulations and avoid the legal and economic repercussions of breaches.

Turn Any Customer Smartphone into a Trusted Authentication Factor
Many financial institutions communicate through reactive messages that only inform the customer about events but don’t give them a chance to respond. Deliver the strongly protected, very convenient and truly native mobile services that customers expect with Push Authentication from DetectID, which sends prompt, interactive alerts that help consumers exercise more control over account management to keep logins safe.

Transition from Legacy Authentication Factors at Your Own Pace
DetectID allows your financial institution to migrate to cheaper, safer and more manageable digital tokens and authentication factors by supporting most of the current form factors and vendors that offer hardware tokens, soft tokens or SMS OTP. DetectID also permits greater deployment flexibility, in which your organization can deploy form factors per channel, user group, or individual user.