VIEW POINT

ADOPT BEHAVIORAL BIOMETRICS AND ANALYTICS FOR EFFECTIVE CYBERSECURITY AND FRAUD MANAGEMENT

Abstract

In recent years, the banking and financial services industry has witnessed increased instances of cybersecurity incidents and online fraud. As per TransUnion's Global Consumer Pulse Study, globally, fraud attempts have escalated by 46% since the onset of the COVID-19 pandemic.[1] This paper offers insights on why and how banks and other concerned financial institutions (FIs), and merchants can leverage behavioral biometrics (BB)-based user entity behavioral analytics (UEBA) solution to effectively combat the burgeoning online fraud and cybersecurity incidents.

Infosys®
Navigate your next

Introduction

Online fraud and cybersecurity incidents have been on the rise at an alarming pace. Factors such as upsurge in digital technology penetration and online payments and transactions, improved savviness and technological advancement of cybercriminals and fraudsters, and increased work from home since the onset of COVID-19, have all led to significant rise in the number of online fraud and cybersecurity incidents. For instance, according to DigitalCommerce360, post COVID-19, there has been massive rise in people's shopping behavior. eCommerce in U.S., for example, rose to by over 5 percent in 2020, as compared to the previous year.[2]

According to a study from LexisNexis Risk Solutions, banks witnessed more fraud attacks per month in 2021 in comparison to the previous year, 2020. The study states that for banks with annual revenue of over USD 10 million, the average monthly fraud attacks volume had increased from 1,977 in 2020 to 2,320 in 2021.[3] According to LogRhythm, 69% of firms have reported incidents of attempted data theft. Also, 81% of the breaches have involved stolen or weak credentials. Further, 91% of the firms report deficient insider threat detection programs.[4]

Today, cyber criminals and fraudsters operate as well-organized rings. They utilize complex methods and automated approaches to perpetrate online crimes. Refer Exhibit 1 for examples of the various online fraud and cybersecurity attacks that criminals have executed in recent times.

Malware (including ransomware)	Advanced persistent threat (APT) attacks	SIM swap fraud	Zero-day exploits	Account takeover
Botnet attacks	Domain Name System (DNS) poisoning attacks	Synthetic identity fraud	Social engineering	SQL injection attacks
Identity theft	Man-in-the-middle (MITM) attacks	Webshell attacks	Point of sale (POS) infiltration	Content injection
Phishing	Whaling	Vishing	Smishing	Spear phishing
Pharming	Cross-Site Scripting (XSS)	Authorized Push Payments (APP)	Visual spoofing	Rootkits
Port scanning	Customer Service Representative (CSR) fraud	IP attacks	Chargeback fraud	Watering hole attacks
DNS spoofing	Brute-force attacks	Cryptojacking	Skimming	Beaconing attacks
Clean fraud	New account fraud	Distributed denial of service (DDoS) attacks	Application fraud	Slow attack
Trojan horse attack	Drive-by attack	DNS tunneling	URL manipulation	IoT-based attacks

Exhibit 1: Examples of cybersecurity attacks and online frauds

For FIs, predicting, identifying, and stopping these online frauds and cybersecurity incidents is extremely challenging. Firms' traditional signature- and rules-based solutions — including firewalls, web gateways, IAM, IDPS, SIEM, EDPR, DLP, and encryption products such as VPNs — have been insufficient to effectively combat today's online frauds and cyber-attacks. For example, these systems:

- Are unable to effectively counter the wide variety of sophisticated online frauds and cyber-attacks being perpetrated today.
- Lack multi-factor authentication capability that are mapped to a user's behavioral profile.
- Apply intrusive authentication methods that increases customer friction and results in poor customer experience.
- Deliver surfeit of false positives which results in reduced efficiency and increased operational cost.
- Unable to offer comprehensive real-time visibility into the firm's network security.

To overcome these challenges and effectively combat online fraud and cybersecurity vulnerabilities, FIs should leverage **behavioral biometrics (BB)-based User and Entity Behavior Analytics (UEBA) solution.**

External Document © 2022 Infosys Limited

Behavioral Biometrics and UEBA: The What and How?

Behavioral biometrics:

Behavioral biometrics relates to a pattern of behavior which is unique to each person. It focuses on the cognitive aspects of an individual such as posture, gait, typing speed, pattern of mouses movement, etc. Refer Exhibit 2 for details on the various types of behavioral biometrics.

In the context of cybersecurity and fraud management, behavioral biometrics technology builds a unique profile for each user, by gathering and analyzing the various behavioral parameters related to how the user interacts with their device or system. The solution starts capturing behavioral information once a user accesses and interacts with the concerned device, website, app, etc. This information is captured in each subsequent interactions of the user across channels and devices. Accordingly, the user's normal behavioral biometrics profile gets built over time.

After the user's baseline behavioral biometrics profile has been created over time, the concerned system would allow continuous and frictionless authentication to the user. For this, system would compare the behavioral biometrics of user's current interactions with the device, website, app, etc. against their baseline behavioral biometrics profile. In case any deviation from the baseline profile is observed, the system would enforce additional step-up authentication for the user.

Behavioral Biometrics Type	Elaboration
Kinesthetics	• **Posture:** unique aspects of a person's body position and weight distribution (while seated or standing). • **Gait:** A person's unique walking style (including upper body posture while walking, stride length, pace of travel).
Voice patterns	• The unique patterns in the sound of a speaker (including pauses, rhythm, pitch variations, etc.)
Device-Based Gestures	• **Keystroke dynamics:** user's unique typing pattern (typing speed, extent of finger pressure while typing, typing rhythm, keystroke duration, typing pauses, etc.) • **Cursor or mouse or cursor movement:** user's unique pattern on trackpad or mouse movement (including tracking speed, paths, clicks, direction changes, etc.) • **Touch characteristics:** User's characteristic movements of touch on a screen, how they tap a touch screen, scroll or swipe pattern, zooming pattern, etc.) • **Holding of phone:** angle at which user holds their phone, the dominant hand with which they use the phone.
Others	• Eye movement and posture, hand-eye coordination, right- or left-handed.

Exhibit 2: Various Types of Behavioral Biometrics

For user authentication, behavioral biometrics is considered superior to physical biometrics. Refer Exhibit 3 for comparison between physical and behavioral biometrics.

Physical Biometrics	Behavioral Biometrics
• Considers inherent static biological characteristics of a user (such as fingerprint, iris pattern, palm, or finger vein).	• Looks at the interactive gestures of user (refer Exhibit 2) and compares those with the user's baseline behavioral gestures.
• Applies single identification point.	• Applies multi-parameter touchpoints.
• Is active in nature; requires active user interaction and special hardware.	• Is passive in nature; analyzes the user's actions in the background for continuous authentication; offers seamless authentication without the need for extra actions from user.
• Is vulnerable to security risks; data can be copied, spoofed, or stolen.	• Is safe; data can't be duplicated as each person has unique behavioral profile.

Exhibit 3: Difference Between Physical and Behavioral Biometrics

External Document © 2022 Infosys Limited

Behavioral analytics and UEBA:

Behavioral analytics involve capturing of qualitative and quantitative data to understand how a user behaves on an app, website, or other digital platforms. By leveraging behavioral analytics capabilities, the solution can predict with accuracy, how the user is likely to act in future. A user's baseline behavioral profile is built over time, based upon each interaction and transaction of the user. In case solution detects deviations in a user's activity from their baseline behavioral profile, it suspects a cybersecurity incident or fraud and undertakes remedial next steps.

User and Entity Behavior Analytics (UEBA) are an advancement to behavior analytics. While behavioral analytics is focused solely on the users, UEBA widens the security perimeter to monitor the activities of both the users and entities (e.g., hardware devices, IoT devices, machines, routers, servers, applications, storage repositories, hosts, IP addresses, endpoints, cloud services, etc.) connected in a firm's IT network. The solution then compares the actual activities of the users and entities to their baseline behavioral profile. In case it detects unusual behavior, it undertakes immediate remedial next steps.

Behavioral Biometrics-Based UEBA Solution: Salient Features

Refer Exhibit 4 for an illustrative list of the data sources that behavioral biometrics (BB)-based UEBA solution typically leverage to support effective cybersecurity and fraud management. Of course, not all data sources would be leveraged by all BB-based UEBA solution. Rather, depending upon a firm's specific cybersecurity and fraud management needs, the solution adopted by the firm would leverage a subset of these and other data sources.

Data Types	Elaboration
Behavioral biometrics data	• Refer Exhibit 2 for the type of behavioral biometrics data that the solution may consider.
Device-related	• Device IP address, type of device used, device make and model, etc.
Location-related	• Location of device from which the user logged in, stated location of user, data from geolocation service providers (such as IP address from HTTP header on order placed at merchant's site by user), etc.
Historical financial data	• User's typical transaction value or spend velocity, user's typical financial transaction activities and pattern across banking channels, etc.
Historical non-financial data	• User's identity information (including the network events that link to the user identity, etc.); usual systems and devices the user logs into; hours and days when the user typically logs in, transacts, or makes payments; user's historic banking cross-channel behavior; usual time spent by user on the site; usual file download size per day; whether the user adds new payees at unusual times; etc.
Transaction-related data	• Time of the current login, transaction amount, to whom payment is made, whether new payee, whether address change was requested, whether request for duplicate card was made, whether password was reset recently, etc.
HR data	• On (ex-employees, employees in notice period, new employees), data on HR incident, etc.
Systems data	• From relevant systems and sources such as core banking system, card system, payments system, lending system, treasury system, accounting system, enterprise applications, ticketing systems, event logs, network flows and packets, web proxy, configuration management databases, network traffic data, VoIP data, etc.
Other security data	• Such as from physical badge access readers, building access card data, external threat intelligence feeds, access systems and logs (e.g., VPN and proxies), authentication systems (e.g., Active Directory (AD)), SIEM, DLP, IDPS, IAM, SOAR, firewall, anti-malware and antivirus systems, EDPR, etc.

Exhibit 4: Data Sources Utilized by BB-Based UEBA Solution

External Document © 2022 Infosys Limited

Refer Exhibit 5 for the key features of robust BB-based UEBA solution.

Feature	Elaboration
Real-time capability	• Offers continuous authentication, and threat detection and prevention in real-time for enhanced cyber security.
Comprehensive	• Ingests and analyzes huge volume of data — from myriad structured and unstructured data sources (refer Exhibit 4) — to build baseline behavioral profiles and unearth anomalies and the potential impact (including blast radius).
Secure	• Behavioral biometrics is difficult to spoof. Also, robust BB-based UEBA solutions are protected with strong security layers.
Risk Scoring	• For any observed deviation of user or entity interaction from their baseline behavioral profile, solution offers accurate predictive risk score in real time — that represents probability of a) the person executing actions being the legitimate user, or b) the entity having been compromised. The higher the risk score of an incident, the greater is the involved cybersecurity or fraud risk. When risk score is beyond acceptable threshold, system automatically enforces additional layers of user authentication, or swiftly undertakes other remedial actions.
Digital capabilities	• Leverages artificial intelligence (AI), machine learning (ML), adaptive behavioral analytics, advanced analytics, and other sophisticated capabilities to enable, for example: o Robust user & entity behavior and threat modeling and analysis (based on relevant data points including external threat intelligence, and the user and entity context). [Note: Solution's ML algorithms can sift through, in real time, the security events and associated data points to detect threats and offer accurate and actionable insights, that signature-based tools otherwise miss.] o Establish context-sensitive baseline for all of the user groups. o Enable dynamic peer groupings of users and entities (such as users from same LoB, or IoT devices of same class). o Substantial reduction in false positives. For this, solution would thoroughly analyze all behavioral, contextual, and other relevant data points, to distinguish false positives from true attacks. Also, solution would not consider an abnormal event solely in isolation, but instead consider the complete context from multiple related signs of abnormal behavior.
User Experience	• Taking a risk-based authentication (RBA) approach, solution would leverage its behavioral biometrics, to offers additional layer of defense in a passive and nonintrusive way, thus reducing friction. The solution won't drive the user's attention away from their task, as relevant data collection and authentication would occur in the background. Only when the solution observes an abnormal behavior, it would enforce additional step-up authentication, and take other necessary actions.
Reporting and dashboards	• The solution would enable sophisticated dashboards and reports that offer, for example: o Intuitive and powerful data visualization. o Visual modelling, visual link analysis, and visual pivoting (on entities for analyzing threat context). o Visual aids for automatic session stitching and timeline analysis. o Ability to quickly drill down into the detailed attack data or on activities performed by an entity or user.

Exhibit 5: Salient Features of Robust BB-Based UEBA Solution

External Document © 2022 Infosys Limited

Behavioral Biometrics-Based UEBA Solution: Key Use Cases in Cybersecurity and Fraud Management

Refer Exhibit 6 for the key use cases in cybersecurity and fraud management of the BB-based UEBA solution.

Exhibit 6: BB-Based UEBA Solution: Key Use Cases in Cybersecurity and Fraud Management

External Document © 2022 Infosys Limited

Refer below the elaboration on each of the use cases mentioned in Exhibit 6 above.

Enable continuous, adaptive & strong customer authentication (SCA)	• Knowledge-based authentication (KBA) are not perfect. For example, a) KBA credentials are easy to gather via social networking, b) crooks can buy hacked credentials information for KBA in black market, and c) KBA slows the user-login process. [Note: KBA requires the person inputting the authentication data to demonstrate knowledge of private information related to the concerned user, to assure the system that the person is indeed the genuine user they claim to be.] • BB-based UEBA solution would: o Enable robust risk scoring. A low-risk score may necessitate simple password challenge. A high-risk score, on the other hand, may lead to three authentication challenges (e.g., password, answering static or dynamic KBA questions, and access code). o Help solve the challenge of 2nd factor authentication by leveraging its risk scoring capability and enabling continuous, adaptive, step-up SCA. o Collect behavioral information (such as speed of OTP entry, how long a key is pressed, etc.) as user processes their SMS OTP for 2nd factor authentication to generate risk score. o Leverage APIs interfaces and ready-to-use connectors to allow bidirectional integration with cybersecurity and fraud risk analytics and the adaptive authentication solutions (to enable a closed-loop for step-up authentication).
Detect and deter insider threats	• An employee, or group of employees, who have gone rogue can utilize their own access to pose insider threats (such as data breaches, patient data snooping, privileged account misuse, etc.). Following categories of people can pose significant insider threat to a firm a) privileged users (e.g., IT administrators), b) knowledge workers (e.g., analysts, developers), c) terminated or resigned employees, d) staff involved in merger or acquisition, e) contractors, f) vendors, and g) partners. • BB-based UEBA solution would continuously monitor and identify the threats posed by negligent, malicious, or compromised insiders. To achieve this, it would utilize its behavioral analytics capabilities and the data from several key sources — including cybersecurity and fraud management systems, security alert logs (from EDPR, DLP, etc.), HR systems and incidents database, physical badge access logs, insider threat databases of the real-world incidents, and more. • In case the solution observes deviation from user's normal baseline behavior it would raise alert or execute automatic mitigation response depending upon the risk score (that, amongst other things, would take into consideration the data criticality, and transaction and resource risk levels). • Following are a few examples of deviations that the solution would flag for insider threats. o Suspicious loan application submission or approvals o Emails forwarded / sent to personal mail ids or to competitor domains o Unusual physical access to sensitive areas o Abnormal password activity o Attempt to login to disabled account o Multiple lockouts and too many authentication failures o Unusual file access and modifications o Unusual login time o Transaction overwrites o New or unusual system access o Deviation from activity patter from self and peer group profiles

External Document © 2022 Infosys Limited

Prevent data exfiltration and IP theft	• BB-based UEBA solution would detect, in real time, malicious or unauthorized data exfiltration, and protect against intellectual property (IP) theft — including incidents such as: o Suspicious data transfers o Sensitive documents downloaded and copied to USB o Abnormal data traffic pattern o Malicious payload drop o Checkout of huge volume of source code from repositories o Emails to personal accounts o Unusual file uploads to cloud storage • To achieve the above, the solution would leverage its ML and behavioral analytics capabilities over the data ingested from myriad sources including DLP and FIM systems.
Detect compromised accounts and privileged access misuse	• A widely used method of cyber-attack is to hijack/compromise privileged user accounts or the trusted hosts connected to a firm's network infrastructure. For example, cybercriminals may get the account owner to unwittingly install malware on their machine, or they may also spoof legitimate account. • BB-based UEBA solution can effectively detect compromised accounts, spoofed accounts, or misuse of high privileged access (HPA) and permission. To achieve this, the solution would: o Leverage its behavioral analytics, deep behavior profiling, and ML capabilities to analyze various parameters such as IP, location, device, timestamp, transaction pattern, access pattern, network packets, etc. o Identify deviation from normal behavior profile of particular account and the associated transactions. o Identify unusual login through Active Directory, cross reference with criticality of device that's being logged onto, sensitiveness of files accessed, and recent malware or unusual network activity that may have led to a compromise. o Automatically monitor and report on unauthorized elevation of permissions or newly created privileged accounts. o Ingest accounts and access data (from IAM, PAM, and directory services platforms), and the activity data (from SIEM, log aggregators, etc.) to a) identify non-HPA accounts that were granted high-privileged entitlements, b) detect shared HPA accounts, and c) unearth and mitigate HPA abuse. o Detect and mitigate shared account usage, and generic account abuse. o Identify anomalous behavior patterns such as: • Access and permission changes on network. • Creation of a super user (note: some attacks involve the usage of super users). • Concurrent logins from multiple locations. • Unusual activity (such as activity from dormant accounts or terminated user accounts). • Account activity from unusual locations or at abnormal time. • Abnormal number of activities from the account. • Abnormal access to high-risk objects. • Accounts having unnecessary permissions.

External Document © 2022 Infosys Limited

Unearth fake accounts	• Cybercriminals have been using fake accounts to perpetrate crime. For example, PayPal revealed that 4.5 million of its accounts were 'illegitimate' and have been shut down as "bad actors" misused its incentives and rewards programs.[5] • BB-based UEBA solution can unearth opening of fake account by verifying identity of the new users based upon their behavior. Note: Real users behave in a different way from fraudsters. For example, real users are: o Often physically present at the location where they state to be living o Less likely to enter their password inaccurately • Fraudsters, on the other hand, while registering a new account, have been known to: o Copy and paste information into account opening or registration forms o Use mobile emulators or apps that wasn't downloaded via official app stores
Bot detection	• Cyber criminals have been making extensive use of bots and bot farms to perpetrate automated attacks. • BB-based UEBA solution would effectively recognize human from bots and take remedial actions. For example, solution can unearth bots that are utilized by fraudster or the firm's competitors to submit 100s of account opening or insurance applications. • To achieve this, the solution would, effectively leverage its behavioral analytics and ML capabilities, and utilize non-PII data and crowd intelligence to: o Differentiate the real traffic from bots — by analyzing user agent attributes such as geolocation, clicks, visits, devices, etc. o Conduct device analysis and ascertain if it is a real device or an emulator. o Automatically evolve existing bot challenges to improve the detection rates. o Enable adaptive bot detection filters that adapt to latest bot attack methods and trends. o Effectively detect and stop unwanted bot traffic to protect mobile apps, websites, and APIs and thwart malicious bot activity such as account takeovers, DDoS attacks, and data scraping.
Account takeover protection	• In Account Takeover (ATO) attack, cybercriminals gain ownership of the online accounts by utilizing stolen usernames and passwords. These cybercriminals usually buy the list of credentials from dark web — the sellers on dark web in turn obtain the credentials through data breaches, social engineering, and phishing attacks. • BB-based UEBA solution can prevent ATO attacks in real time. For this, the solution would: o Leverage its behavioral analytics capabilities to continuously monitor the users' activity patterns and identify anomalous activities, such as: ▪ Transactions executed from unusual location. ▪ Payment requests of large sum to previously unknown account. ▪ Not in line with user's usual location behavior. o Raise immediate alert, or trigger step-up-authentication, or block access to the user — in case the solution deems that the user's activity is high-risk and potentially fraudulent. • Thus, even if the attacker has managed to attain sensitive information (e.g., username and password) or the second-factor authentication code, they won't succeed in account takeover.

External Document © 2022 Infosys Limited

SIM swap fraud prevention

- In SIM swap fraud, criminals fraudulently get the victims' cell numbers transferred to their own SIM cards. As a result, the crook gains access to text messages, incoming calls, and security prompts that are sent to the victim's mobile number. They then utilize such confidential information to gain access to victim's account, system, etc.
- BB-based UEBA solution would:
  - o Leverage device intelligence, user's stated location, and other relevant behavioral biometrics and analytics data points, in real time, to ascertain whether the person accessing the FI's app, website, or system is genuine or a crook.
  - o Compare the user's current activity pattern with the user's established behavioral profile.
- As a result, even if the fraudster has gained access to the victim's credentials and authentication SMS code, solution would reveal that the current behavior is inconsistent with the legitimate user's past behavioral pattern, an accordingly take remedial actions.

Synthetic identity fraud detection and prevention

- In synthetic identity fraud, criminals create a fake persona by making use of a combination of real, manufactured, or stolen PII.
- BB-based UEBA solution can identify, in real time, synthetic identity fraud — for example, during account opening (for personal loan, credit card, etc.) or at the time of new insurance policy creation. To achieve this, system would:
  - o Leverage deep behavioral biometrics and analytics capabilities to ascertain:
    - How the user physically interacts with their computer or mobile device.
    - How familiar with their PII does the user appear while entering PII info (such as name, DOB, SSN, email id, address, phone number, etc.)
  - o Analyze user's behavior vis-à-vis the high-risk behaviors known to be associated with synthetic ID fraud (during account creation application), such as:
    - Copy and pasting of the PII (where fraudster typically uses a list of synthetic IDs for opening multiple accounts).
    - Moving very quickly through various data entry fields. Note: This is because the fraudster is well-versed with the process as they have completed the said application process several times in the past for perpetrating synthetic ID fraud.
    - Usage of advanced navigation and shortcut keys (that aren't usually utilized by typical users).
    - Usage of bots for automated completion of applications.

External Document © 2022 Infosys Limited

Customer Service Representative (CSR) fraud detection and prevention	• CSR fraud is a type of insider fraud in which insiders in the customer service group of an organization are involved. These insiders, who have privileged access to a broad range of customer accounts, perform fraudulent activities vis-a-vis those accounts. • BB-based solution would ingest data from numerous sources — including VoIP phone data, ticketing systems, badge access data, network events, and workstation events that link to user identity — to detect CSR fraud scenarios such as: o Unusual activity pattern o Abnormal data transfer o Customer profile changes without associated service request or ticket o Abnormal session time o Malicious out-bound / in-bound phone activity
Tackle insurance fraud	• As per FBI, annual insurance fraud (non-health) losses are ~US$ 40 billion — which costs average American family US$400-US$700 in increased insurance premiums each year.[6] Cybercriminals, for example, get fraudulent insurance account created using stolen data. They may even misappropriate real insurance account of legitimate users. Post that, criminals may get away with diverted insurance payments or false insurance claims for days or even weeks before the fraud gets detected. A key shortcoming of insurance firms — which cybercriminals exploit — is their overreliance on PII data for customer verification. Data breaches make such PII available to fraudsters (for e.g., through sale on dark web). Fraudsters can then combine such real data with fabricated data to create 'synthetic' online identities. • BB-based UEBA solution would leverage its behavioral analytics capabilities and help combat insurance fraud by: o Leveraging shared intelligence on known insurance frauds. o Unearthing, in real-time, suspect behavioral biometrics and other signals within a customer's session during insurance policy application and creation, or during other insurance related transactions. o Identifying synthetic identity fraud during new insurance policy creation. o Identifying usage of bots (by a fraudster or competitor) to submit 100s of insurance policy applications.
Detect and prevent other complex frauds	• BB-based UEBA solution can effectively leverage its behavioral analytics capabilities to promptly detect other types of online frauds such as: o Application fraud (by performing continual checks during the application process). o New account fraud (by comparing the user's behavior (e.g., spending behavior, sequence of actions, etc.) against the representative customer pool).

External Document © 2022 Infosys Limited

Enforcement of zero trust policy

- Zero Trust Architecture (ZTA, aka perimeterless security) is a security framework that requires all users (whether outside or inside the firm's network) to be authenticated, authorized, and constantly validated for being granted or to retain access to the concerned data and applications. The underlying principle of ZTA is "never trust, always verify" — i.e., a device shouldn't be trusted by default even if it is connected to a permissioned network (e.g., corporate LAN) and even if the device was already previously verified.
- To support the enforcement of ZTA, BB-based UEBA solution would:
  - Enable ongoing monitoring of all devices and users connected to the network.
  - Leverage its behavioral analytics capabilities to evaluate security risks such as:
    - Whether a trusted entity or user is behaving abnormally.
    - Whether zero trust policies are being broken.
    - If a new device is connected to the network.
    - Whether a user is trying to connect with services that are outside of their privileges.
  - In case security risks are observed, the solution would execute one or more actions such as a) sending alert to SOC, b) triggering automated response (e.g., suspension of suspicious activity, isolation of user account).

Unearth of cloud security vulnerabilities

- BB-based UEBA solution can leverage relevant data sources of the cloud infrastructure and effectively utilize its behavioral analytics capabilities to unearth cloud security issues such as:
  - Unauthorized login and access
  - Suspicious transmissions
  - Anomalous data sharing
  - Privilege access misuse
  - Data exfiltration
  - External attacks from beyond the cloud

Discovery of Internet of Things (IoT) security risks

- Firms typically deploy huge number of connected devices to support their day-to-day operations. Cybercriminals can compromise such IoT devices, and gain access to the firm's IT systems and steal sensitive data. They may even leverage these IoT devices to execute DDoS attacks against 3rd parties.
- BB-based UEBA solution would:
  - Effectively track the connected devices in real time.
  - Build behavioral baseline for every device or group of similar devices.
  - Promptly discover if a device is behaving abnormally, such as:
    - Connections to or from unusual devices or addresses.
    - Device features that aren't normally used got activated.
    - Activity at unusual times.

External Document © 2022 Infosys Limited

Network lateral movement detection

- Network lateral movement (aka lateral movement) is a technique used by cybercriminals and adversaries to extend access to other applications or hosts or in a firm, after the firm's endpoint has been compromised. Lateral movement allows the cybercriminal or adversary to maintain persistence in the network, and a) move nearer to valuable assets of the firm, or b) allow the cybercriminal or adversaries to gain control of an administrator's system and the data and privileges associated with it. In lateral movement, the attack moves laterally through a firm by changing IP addresses, credentials, or machines. Examples of lateral movement include a) pass the ticket (PtT), b) pass the hash (PtH), c) internal spearphishing, d) exploitation of remote services, f) windows admin shares, g) SSH hijacking.
- BB-based UEBA solution would leverage its behavioral analytics capabilities to detect lateral movement (as this type of attack would nearly always force the attacked network entities and assets to behave differently from their established baselines). To detect lateral movement, the solution would:
  - Leverage its integration with SOAR solution to quickly identify and respond to lateral movement and all associated malicious activities — thereby reducing the likelihood of a threat actor moving across the network and gaining access to sensitive system and data.
  - Automatically combine insights on behavior, identity, sequence, and scope to:
    - Offer a unified view of the entire network operation.
    - Stitch together associated security events to offer complete timeline of composite security incident (spanning multiple IP addresses, users, event streams, devices, and IT assets).
    - Assign risk score to the composite security incident.
    - Tie data from myriad sources to offer visibility in the attacker's journey within the network.

Combat social engineering

- Social engineering attacks involve the usage of deception to manipulate persons into revealing personal or confidential information that may be utilized for fraudulent purposes. Examples of social engineering include phishing, baiting, spear phishing, whaling, scareware, vishing, watering hole, pretexting, and pharming.
- BB-based UEBA solution would work along with SIEM solution to speedily detect and respond to social engineering attacks. The solution would:
  - Gather security events and logs from across relevant sources to establish normal behavior profile of individuals, groups, end devices, etc.
  - Leverage behavioral analytics to identify deviations in behavior from normal behavioral profile.
  - Leverage behavioral biometrics and analytics insights on the user to unearth in case the user is unknowingly interacting the cybercriminal. Solution can suspect such interactions by identifying user behavior such as:
    - Demonstrating hesitant behavior (because the user has reservation on what they are doing).
    - Taking unusually long pauses (maybe because the user is waiting for further instruction from the cybercriminal).
    - Picking and putting down their mobile phone intermittently (maybe because the user is in back-and-forth calls with the criminal who is giving direction on the next steps).
  - Proactively intervene and alert the victim to not engage further — in case a cybercriminal has already succeeded in gaining trust of the unsuspecting victim.
  - React using automated incident response playbooks to prevent or minimize damage.

External Document © 2022 Infosys Limited

Detect slow-and-low attacks

- Many cybersecurity events that may otherwise look harmless in isolation can turn out to be high-risk threats when analyzed in the larger context over time.
- BB-based UEBA solution would:
  - Effectively correlate and analyze cybersecurity events, over time, using data from multiple sources (including devices, assets, users, applications, and network segment).
  - Predict, detect, and mitigate the slow-and-low attacks that are otherwise not apparent in isolation to traditional cybersecurity solutions.
  - Leverage ML algorithms along with databases that offer industry intelligence on slow-and-low attacks to identify the specific type and mode of the attack.

Cyber threat hunting & identification of other cybersecurity risks

- BB-based UEBA solution would leverage its behavioral biometrics and analytics capabilities for speedy cyber threat hunting and identification of several other cybersecurity risks, such as:

Ransomware attack	Malware attack (viruses, backdoors, trojans, RATs, rootkits)	SQL injections
DDoS attack	Advanced Persistent Threat (APT)	DGA attack
Zero-day attack	Beaconing attack	Brute force attack
Replay attack	MITM attacks	DNS tunneling attack

Stateful session tracking

- BB-based UEBA solution would:
  - Help effectively build and track the user session state — even when the user navigates across heterogeneous applications or resources using different devices and accounts at different times.
  - Leverage its ML capabilities to dynamically build session correlation attributes (utilized for building session context for linking subsequent activities).
  - Enable identification of valid IP switching (due to transitions between workstation and mobile device, or wireless and wired networks, or for accessing enterprise resources remotely over the VPN or from various onsite locations).
  - Highlight anomalous activity from a user session or the concurrent sessions from same account.
  - Help expedite the detection of session replay and session hijacking attacks.
  - Deliver high visibility into sequence of events.
  - Significantly reduce the false positives associated with common scenarios such as IP, device and account switching while performing day-to-day activities.

External Document © 2022 Infosys Limited

Support for self-audit	• BB-based UEBA solution would offers robust cybersecurity self-audit support to the users and security managers. For this, solution would leverage its behavioral analytics and ML capabilities to offer actionable contextual insights (on users, entities, accounts, devices, applications, systems, data, etc.) — that are otherwise not offered by traditional cybersecurity solution.
Incident prioritization	• A common challenge faced by SOC with traditional DLP and SIEM is that these solution (that are typically rule- and signature-based) generate large number of alerts, many of which are false alerts. This adversely impacts the SOC analysts in incident prioritization. • BB-based UEBA solution would: o Leverage its behavioral analytics and ML capabilities to detect the unknown. o Offer risk scoring to help understand which incidents are potentially dangerous or especially suspicious. o Aggregate the risk scores at entity and user level, instead of generating huge number of alerts at event or transaction level. o Go beyond the traditional threat models to leverage additional unique data types (such as criticality of assets, and access levels of a particular organizational function) to prioritize incidents. For example, even a small deviation from the baseline behavioral profile for a high-level administrator or a critical system may indicate a high-priority incident. On the other hand, for a junior employee with limited access to the firm's network and zero access to key systems, even if the deviation from baseline profile is large, it need not necessarily be a high-priority incident. o Take SIEM and DLP alerts and help prioritize and consolidate by leveraging its behavioral analytics capabilities. (Note: BB-based UEBA solution would leverage its bidirectional integration (using APIs) with the SIEM and DLP tools; thereby enabling effective data and alert ingestion into the solution. Solution would also enable the exportation of risk scores to SIEM and DLP tools.)

Behavioral Biometrics-Based UEBA Solution: Key Implementation Considerations for FIs

In undertaking to implement robust BB-based UEBA solution, FIs must take heed of certain key implementation considerations — Refer Exhibit 7.

Exhibit 7: Key Implementation Consideration for Robust BB-Based UEBA Solution Implementation

External Document © 2022 Infosys Limited

Leverage advanced analytics and AI/ML capabilities

Some UEBA solutions predominantly rely on manually defined rules to identify the suspicious activities. Resultantly, these solutions are only as good as their defined rules. Moreover, these solutions are unable to adapt to new varieties of cybersecurity threats or frauds.

To make sure that they don't face such challenges, FIs must ensure that the BB-based UEBA solution they adopt possess robust advanced analytics, artificial intelligence (AI), and machine learning (ML) capabilities. By utilizing such new-age capabilities, the BB-based UEBA solution would be able to:

- Leverage variety of sophisticated ML algorithms, library of threat models, and huge volume and vast array of data sources to enable high effectiveness.
- Offer real-time and adaptive monitoring and analysis (of threat, event rarity, network, peer group, impact, and more).
- Enable thorough stitching together of threat indicators to offer accurate threat detection, risk scoring, and impact assessment (including for new and never seen before threats).

Refer Exhibit 8 for some of the sophisticated ML algorithms that the new-age solutions leverage to offer optimal benefits. Refer Exhibit 9 for an illustrative high-level functional architecture of digitalized BB-based UEBA solution.

Supervised ML	Logistic Regression, Linear Regression, Neural Networks, Decision Trees (e.g., ID3, C4.5, CART, BehavDT, IntrudTree), RNN, Naïve Bayes.
Unsupervised ML	K-Means, Hierarchical Clustering, DBSCAN, LOF, One-Class SVM.

Exhibit 8: Illustrative ML Algorithms Utilized by BB-Based UEBA Solution

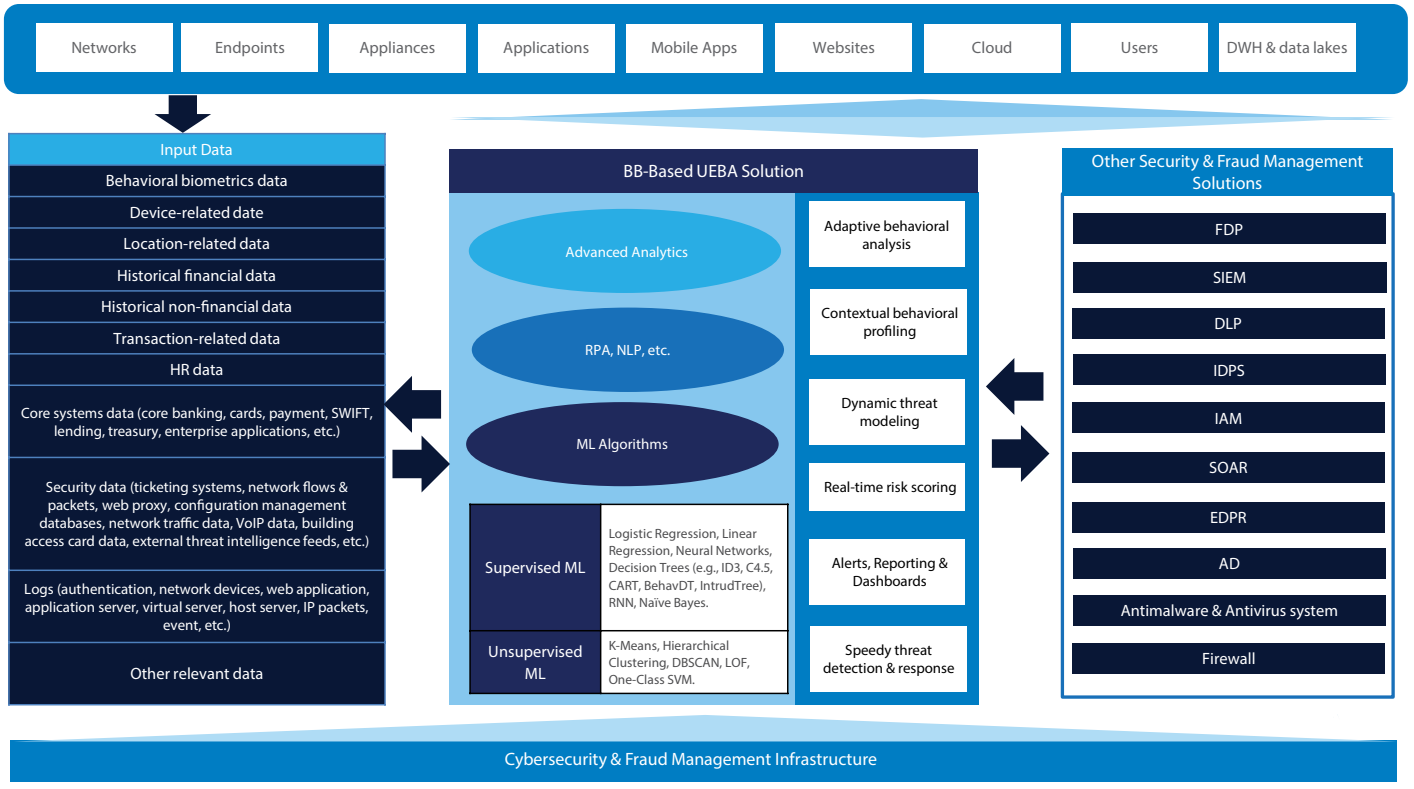

Exhibit 9: Illustrative High-Level Functional Architecture of Digitalized BB-Based UEBA Solution

External Document © 2022 Infosys Limited

Ensure robust integration

FIs should not make the mistake of considering BB-based UEBA solution as a substitute for their other traditional but essential cybersecurity and fraud management systems. Rather, the BB-based UEBA solution should be viewed as a strong complement to the traditional systems.

BB-based UEBA solution should therefore be well integrated with the firm's key cybersecurity, fraud management and other relevant systems, including:

- Identity and access management (IAM) system
- Intrusion Detection and Prevention System (IDPS)
- Security information and event management (SIEM) solution
- Endpoint Detection, Protection and Response (EDPR) system
- Security orchestration, automation, and response (SOAR) solution
- Active Directory (AD)
- Data Loss Prevention (DLP) system
- Anti-malware and antivirus systems
- Other core systems (such as CBS, payments system, SWIFT system, lending system, HR system, etc.)
- Relevant big data platforms, data warehouses and data lake, and data sources

To highlight the importance of integration, consider SIEM systems — these systems support threat detection and security incident management through collection and analysis of security and associated events and the contextual data. Traditionally, SIEM systems have lacked behavioral analytics capabilities. Instead, they discover threats using user-defined correlation rules. BB-based UEBA solution integration with SIEM solution can address this gap — it would allow the harvesting of the breadth of data in SIEM using the behavioral analytics capabilities of UEBA engines.

As another example to highlight the importance of robust integration, consider SIEM, AD and DLP solutions. Robust integration would enable these solutions to offer key data from relevant sources to the BB-based UEBA. This would enable additional context (vis-a-vis identity profile information, access grants, and activity and alerts from applications) to the BB-based UEBA solution. As one more example, UEBA solutions that are well-integrated with SOAR solution would allow the SOC team to quickly identify and respond to malicious activities.

Focus on data privacy

It is important for FIs to ensure that their BB-based UEBA solution implementation don't compromise on data pricacy. For example, the solution:

- Should not gather and store personally identifiable information (PII), username or password and violate any relevant data privacy laws.
- Should not store or analyze the actual content typed by the user or the details of transactions executed. Instead, it should only capture the patterns of users' micro-behavior (such as typing speed, how the keys were pressed, etc.) and the other relevant data points essential for its security monitoring and analysis.
- Ensure appropriate levels of encryption and data masking while leveraging contextual behavior data — so as to protect the users' identities.

Also, FIs must take due care while implementing the solution for mobile devices. This is because mobile behavioral analytics are much more intimate than other devices such as desktop. For example, mobiles involve many more sensors (e.g., gyro, accel, and touch). Data from these sensors, when analyzed, can reveal highly personal insights on a user's daily life (for e.g., what time the user wakes up or goes to bed, what time they leave for work, etc.). Storing such private user information on centralized servers can lead to massive breach of user security and privacy. Hence, FIs must work on implementing decentralized sensor-based contact tracing by leveraging relevant AI and ML algorithms on-device. This would prevent sensitive user data to leave the mobile device, thereby promoting decentralization and bolstering user's privacy. Also, firms must ensure that appropriate hardware-level encryption are enforced on the mobile devices.

External Document © 2022 Infosys Limited

Embrace holistic approach

For BB-based UEBA solution to be truly effective, it is important that firms undertake a holistic approach. For example, depending upon their specific security needs, firms may need to ensure:

- UEBA capabilities are installed on all devices connected to the network or used by employees — including the devices owned by the employee and which get connected to the organization's network.
- Employees install relevant BB-based UEBA capability on their home routers as well, as the routers can also be a threat vector for the organization.
- Non-privileged user accounts are not treated as harmless. This is because, attackers usually gain control of such standard accounts and escalate the privileges to infiltrate sensitive systems.
- Robust and reliable fallback authentication mechanism — that can cater to relevant exceptions and also can't be misused by cybercriminals — are implemented. This is because BB-based UEBA solution may not work all the time. For example, in case a user faces temporary injury to a hand, and therefore uses the 'weaker' hand to complete OTP. This would adversely impact the user's behavioral profile, and resultantly system may not allow this genuine user to proceed further.
- Alternate authentication mechanisms are enabled for users until sufficient data on their behavior has been gathered to allow behavioral biometric-based identification. For example, for users that access the secured systems infrequently (e.g., only once or twice a year), it would take long for system to build their baseline behavioral profile to allow them behavioral biometrics-based authentication.
- Solution has mechanism in place to exclude confirmed fraudulent events from the behavioral profiles. This is crucial to ensure that future authentication attempts and transactions by legitimate users are not adversely impacted.
- Solution takes device-switching scenarios into consideration and build user profiles accordingly. This is because, many users shop using both desktop/laptop and on mobile. For such users, switching between devices may yield different behavioral patterns.
- For authentication decisions, solution takes into consideration additional key factors unique to the user (e.g., user's location). Such additional considerations would help bolster decision confidence for SCA and also improve overall authentication rates.
- Solution does not base its insight on geolocation using IP addresses alone. This is because criminals can spoof their location (using VPNs and proxies) and fool the systems that utilize simplistic location models such as IP address.
- Granular, role-based access control is enforced, and that access and entitlements to data are strictly as per business needs.
- Each facet of the BB-based UEBA solution and the overall cybersecurity and fraud management infrastructure is regularly tested and updated (as needed). This is because criminals are constantly improving their attack techniques and therefore firms need to remain a step ahead.

Solution vendor due diligence

Vendor solutions in the BB-based UEBA space vary significantly in terms of capabilities, type, and quality of offerings. For example, standalone BB-based UEBA solutions are available for deployment in on-premises as well as in cloud-based mode. Also, solution vendors may have their specific implementation criteria, such as a) requiring the adopting firm to deploy software for core components of the solution, b) deploying appliances (virtual or physical) for monitoring endpoint agents and network traffic, c) specific requirements vis-à-vis data platforms (e.g., requiring that data is sent to a standalone data lake that is managed by vendor), etc. Also, vendors' strategy vis-à-vis key aspects such as end-to-end management and governance (related to ensuring data and session privacy, data quality etc.) may vary.

Hence, it is imperative that FIs analyze in detail the vendors' solution offerings, implementation criteria, end-to-end management, etc. and select the solution that strongly aligns with the their specific needs.

External Document © 2022 Infosys Limited

Sensible adoption strategy

Standalone UEBA solutions are usually implemented by large global firms that have complex and evolving security needs. This is because, UEBA solutions are costly to purchase, implement, maintain, and use. Therefore, firms planing to leverage BB-based UEBA solution must conduct thorough cost benefit analysis. They should adopt a full-fledged solution only if they have compelling reasons for it (for example, as part of the firm's new comprehensive insider threat protection program, or to substantially augment and bolster the firm's existing SIEM solution). Small and medium-sized firms should explore alternative approaches — such as adopting or upgrading other point or traditional solutions (such as IDPS, SIEM, EDPR, SOAR, DLP, firewalls, web gateways, and VPNs, etc.) — to see if their evolved cybersecurity and fraud management needs can be met.

Further, as stated earlier, BB-based UEBA implementation are computationally expensive and data-intensive. Hence, to reduce these costs firms should strategize and only capture the crucial data points, rather than blindly gathering all of the users and entity interactions in a network.

Also, when implementing BB-based UEBA solution, firms should start small rather than adopting a "big bang approach". For example, the initial implementation of the solution should be restricted to limited data sets and a narrow range of well-defined use cases. Such an approach will help gauge the feedback from the initial implementation, finetune the approach and models, and after improved performance, gradually expand the implementation to more data sets and new use cases.

Behavioral Biometrics and Behavioral Analytics Implementation: Real World Examples

Entity	Elaboration
TransUnion & Neuro-ID[7]	• Neuro-ID is a next-gen provider of real-time behavioral analytics. It leverages rich behavioral data sources; data is collected in real-time from any device. • TransUnion and Neuro-ID partnered to help insurance industry detect fraud, support customers, and improve CX. TransUnion is leveraging Neuro-ID's Friction Index Platform and Fraud Solutions for its insurance customers — to better the customer experience, reduce friction, and identify behavioral risk and fraud. Neuro-ID's Friction Index Platform uncovers points of friction, confidence and hesitation as the applicants interact digitally with an online claim or quote or claim process.
Zelle[8]	• Zelle — a P2P payment platform — enables its bank purveyors to analyze over 2,000 behavioral risk indicators in real-time, and detect anomalies in a legitimate user's behavior, navigation, patterns, location, and several other tell-tale signals that point to potential fraud.
Entersekt / Capitec Bank[9, 10]	• Entersekt has partnered with Capitec Bank (amongst the largest retail banks in South Africa) to improve security and decrease friction for e-commerce transactions. By employing Entersekt's EMV 3-D Secure solution, Capitec can recognize, in real time, high-risk e-commerce interactions. Entersekt's EMV 3-D Secure solution blends strong authentication capabilities with modern behavioral technology to tackle security issue. • Entersekt's solution utilizes behavioral analytics from NuData Security (a Mastercard firm offering advanced risk-based authentication technology). NuData incorporates behavioral biometrics and ML capabilities, and insights from billions of anonymous data points (including on identity, device, geolocation) to differentiate between potential fraudsters and genuine users — based on their mobile app, online, and smartphone interactions. The solution enables a risk score for the cardholder's e-commerce transaction during checkout. • If the risk score is low, user continues to have frictionless authentication experience. However, when risk score is high (denoting a high-risk case), step-up authentication process gets triggered. The solution supports several authentication methods, including biometrics, in-app push prompts, and FIDO-certified security keys. The behavioral analytics offered by NuData Security also enables Entersekt to identify devices which have been flagged for fraud at another bank. This makes it easier for different FIs to collaborate on combatting fraud.

External Document © 2022 Infosys Limited

FICO[11]	• FICO acquired EZMCOM (a behavioral biometrics provider, whose products are utilized by banks globally to protect over 60 million customers from account takeover, identity theft, and breaches). • Two products ensuing from the integration, and now part of FICO platform for authentication and identity proofing, are: a) FICO Identity Proofing (for digital onboarding), and b) FICO Authentication Suite (that comprises biometric, multifactor, and behavioral authentication). The products support eKYC, digital onboarding, and PSD2 mandated SCA to manage risk. • FICO Identity Proofing verifies customer identity by utilizing an AI-powered biometric analysis of a government ID photo and a selfie. The solution runs liveness tests to thwart spoofing. • FICO Authentication Suite performs device telemetry and keystroke analysis to verify genuine customers. It also leverages ML algorithm combined with biometrics to reduce the chances of account takeover.
TypingDNA[12]	• TypingDNA has introduced continuous biometric authentication for the remote workers, and support enterprise zero trust cybersecurity strategies. Its ActiveLock solution leverages the firm's typing biometrics capabilities to authenticate users seamlessly, using non-intrusive analysis of the users' typing patterns. If it detects an unauthorized user, it sends out alerts or locks the device in real-time. The solution is privacy-preserving — it doesn't analyze the typed content.
Feedzai[13]	• Feedzai acquired Revelock — the acquisition has created the world's biggest AI-powered financial risk management platform with integrated and native behavioral biometrics. The acquisition has resulted in the world's largest Financial Intelligence Network (FIN), a vault of over trillion data points, sessions, and profiles of good and bad actors. • The platform enables pre-transaction behavioral intelligence, in real time, for banks, acquirers, payment processors, and merchants. It helps promptly spot and prevent financial crime before they occur and without compromising user experience or privacy. Apart from behavioral biometric data, the solution leverages AI and ML capabilities for predictive intelligence to thwart financial crime in real-time. • Feedzai's segment-of-one profiles leverage 50B data points to decide whether a transaction is fraudulent. In addition, Revelock brings in biometric intelligence from every device, session, and user that connects to the system. Revelock technology bolsters Feedzai's platform capabilities by offering robust digital identity solution that leverages advanced behavioral analytics solution powered by deep learning. Revelock's technology can detect subtle changes in user's behavior — such as how quickly they navigate a banking app, or how they hold their phone — to confidently predict whether a session is fraudulent.
Kount[14]	• Kount launched adaptive protection solution — that leverages behavioral biometrics, rich login data, and policy customization — to avert account takeover fraud. The customizable and unified solution helps combat malicious bots, logins, brute force attacks, and credential stuffing while enabling enriched and personalized customer experience through adaptive friction. The solution analyzes, in real time, the user behavior and anomalies at network and device level to detect high-risk login activity. Kount has a relationship with BehavioSec to integrate behavioral biometrics such as keystroke dynamics into its fraud management products.
LexisNexis Risk Solutions[15]	• LexisNexis Risk Solutions acquired BehavioSec for behavioral biometrics. BehavioSec leverages its predictive behavioral biometrics solution for continuous authentication for establishing identity trust and preventing fraud. It converts mobile signals from sensors and touchscreen into advanced mobile behavioral biometric-based authentication capabilities. The integration of offerings from BehavioSec into the LexisNexis ThreatMetrix will benefit customers by enabling advanced ML capabilities, utilizing additional behavioral data for enhanced authentication, and supporting continuous authentication.
BioCatch[16]	• BioCatch launched behavioral biometrics solution to help thwart fraudulent account openings that target the vulnerable and elderly. The solution, Age Analysis, leverages behavioral biometrics to safeguard against myriad application frauds related to attempted account openings for credit cards. It empowers FIs with behavioral verification protections.

External Document © 2022 Infosys Limited

BioCatch[17]	• BioCatch has an approved patent on behavioral biometrics enabled Mule Account Detection solution. The patent illustrates a solution that is designed to identify mule bank accounts utilized for terror funding or money laundering. The solution leverages real-time monitoring tools to evaluate user behavior when they access online banking account. • The solution can identify five different personas that are commonly linked with mule accounts, including a) accounts clearly created for muling money, b) genuine accounts that criminals take control of and then utilize to funnel money, c) fraudsters who pay students to leave their empty accounts after completing their course, d) individuals who unknowingly or knowingly share their bank accounts with crooks.
Mastercard[18,19]	• Mastercard launched an integrated product suite to offer healthcare partners tools for fraud detection, protection of data on patient health, and efficient service delivery. The solutions offer a combination of biometrics and behavioral analytics to safeguard health information, and AI and ML capabilities to identify suspicious claims activity. • Amongst cybersecurity products in the suite, NuDetect solution leverages behavioral biometrics, and 100s of anonymized user data points, to offer continuous verification. • Leveraging biometrics, behavioral analytics, and risk assessment capabilities, Mastercard Healthcare Solutions can a) authenticate mobile access to HSA accounts, patient portals, and call centers, b) detect cybersecurity threats in real-time, c) mitigate data exposure and automated cyberattacks mobile apps and websites, d) identify ID management and security gaps, and e) dependably authenticate patients during the new account enrollment.
Ping Identity[20]	• Ping Identity acquired SecuredTouch to leverage its bot detection and behavioral biometrics capabilities to offer more secure and seamless experiences to enterprise customers. By integrating SecuredTouch within PingOne Cloud Platform, enterprises would gain access to advanced signals, intelligence, and data that can leverage behavioral biometrics for step-up authentication and for understanding fraudsters' behavior to combat malicious behavior such as emulators, bots, and account takeover.
BlackBerry[21]	• BlackBerry had unveiled a new UEBA solution (called Persona Desktop) for real-time identity verification and continuous biometric authentication to stop security breaches. The solution, which leverages AI and ML capabilities, is built on BlackBerry Spark Platform. It analyzes users' interactions with their devices to ascertain security risk. User actions that go beyond the risk threshold result in instant alerts which triggers the user for second-factor authentication. The solution leverages typing biometric data such as mouse gestures and keystrokes to recognize a different user and trigger alerts or lock the device.
NatWest[22]	• NatWest has been leveraging Featurespace's ARIC Risk Hub for payments fraud detection and enterprise-wide AML transaction monitoring. Featurespace's ARIC Risk Hub leverages behavioral biometrics and adaptive behavioral analytics to monitor individual behavioral activity in real-time and protect customers from Authorized Push Payments (APPs) and other threats.
Aetna[23]	• Insurance giant Aetna Inc. implemented security measure, that monitors user behavior in real time, for its web and mobile applications. • Rather than depending only on fingerprint or password entered at a single point in time, Aetna apps constantly monitor the security based upon user behavior and several other contextual clues, such as location. Attributes such as device configuration, apps used most frequently by the user, how the user holds their phone, are fed into a risk engine that leverages ML to generate individual risk score for each user. When a user's actions deviate substantially from their baseline normal behavior, the risk level rises, and the app may demand another form of authentication from the user before they can proceed further or may restrict access to certain functions.
Jack Henry & Associates (JHA) and NuData Security[24]	• Jack Henry & Associates (JHA, a leading provider of technology solutions and payment processing services chiefly for the financial services industry) partnered with NuData Security (a Mastercard company) to enhance JHA's Banno Digital Platform with behavioral technology to recognize, in real-time, high-risk users during login. The technology leverages behavioral analytics, passive biometrics, enhanced device recognition capability, and cloud-based trust consortium. • NuData Security solution leverages ML to continuously update signals, modules, and rules with billions of analyzed data points. It successfully blocks over 99% of automated account takeover and credential testing attempts, thereby helping prevent account takeover, credential stuffing, application fraud, transaction fraud, and other threats.
Featurespace[25]	• Featurespace had launched Automated Deep Behavioral Networks for card and payments industry. The next-gen ML solution — which leverages RNNs available through new version of Featurespace's ARIC Risk Hub — offers a deeper layer of defense against account takeover, scams, and card and payments fraud.

External Document © 2022 Infosys Limited

Conclusion

According to U.S. Federal Trade Commission (FTC), in 2021, consumers had lost US$5.8 billion to fraud amounting to 70% rise from the previous year.[26] The cost of a data breach had risen by 10% in 2021, reaching US$4.24 million per incident.[27] As more individuals and businesses adopt digital channels, fraud and cybersecurity risks are expected to continue to rise substantially.

To effectively combat such increasing risks, FIs should leverage multilayered security stack of which robust BB-based UEBA solution must form a key component. Behavioral biometrics and UEBA technologies have immense potential. It is therefore not a surprise that global behavioral biometrics market is projected to reach USD 3.91 billion by 2026 — rising at CAGR of 25.62% between 2021-2026.[28] And, that the global market for UEBA is projected to be worth US$4.2 Billion by 2026 — growing at CAGR of 39.2% between 2020-2026.[29]

Acronyms

Acronym	Expansion	Acronym	Expansion
AD	Active Directory	LAN	Local Area Network
AI	Artificial Intelligence	LoB	Line of Business
AML	Anti-Money Laundering	LOF	Local Outlier Factor
API	Application Programming Interface	MFA	Multi-Factor Authentication
APP	Authorized Push Payment	MiTM	Man-in-the-Middle
APT	Advanced Persistent Threat	DLP	Data Loss Prevention
ATO	Account Takeover	DOB	Date of Birth
CAGR	Compound Annual Growth Rate	FIM	File Integrity Monitoring

External Document © 2022 Infosys Limited

CART	Classification And Regression Trees	ML	Machine Learning
CBS	Core Banking System	NLP	Natural Language Processing
CSR	Customer Service Representative	OTP	One-Time Password
CX	Customer Experience	P2P	Peer-to-Peer
CVSS	Common Vulnerability Scoring System	PAM	Privileged Access Management
DBSCAN	Density-based Spatial Clustering of Application with Noise	PII	Personal Identifiable Information
DDoS	Distributed Denial-of-Service	POS	Point of Sale
DGA	Domain Generation Algorithm	PSD2	Payment Services Directive 2
DNS	Domain Name System	PtH	Pass-the-Hash
DWH	Data Warehouse	PtT	Pass-the-Token
EDPR	Endpoint Detection, Protection and Response	RAT	Remote Access Trojan
EPP	Endpoint Protection Platform	RBA	Risk-Based Authentication
eKYC	Electronic Know Your Customer	RNN	Recurrent Neural Network
EMV	Europay, MasterCard, and Visa	RPA	Robotic Process Automation
FDP	Fraud Detection & Prevention	SaaS	Software as a Service
FI	Financial Institution	SCA	Strong Customer Authentication
FIDO	Fast IDentity Online	SIEM	Security Information and Event Management
FIM	File Integrity Monitoring	SIM	Subscriber Identity Module
FTC	Federal Trade Commission	SOAR	Security Orchestration, Automation, and Response
HPA	High Privileged Access	SMS	Short Message Service
HR	Human Resources	SOC	Security Operations Center
HSA	Health Savings Account	SSH	Secure Shell
HTTP	Hypertext Transfer Protocol	SSN	Social Security Number
IAM	Identity and Access Management	SWIFT	Society for Worldwide Interbank Financial Telecommunication
IDPS	Intrusion Detection and Prevention Systems	UEBA	User Entity Behavioral Analytics
IDS	Intrusion Detection System	UI	User Interface
IOC	Indicator of Compromise	USB	Universal Serial Bus
IoT	Internet of Things	VoIP	Voice over Internet Protocol
IP	Internet Protocol	VPN	Virtual Private Network
IP	Intellectual Property	XSS	Cross-Site Scripting
KBA	Knowledge-Based Authentication	ZTA	Zero Trust Architecture

About the Authors

Anjani Kumar

Principal Consultant, Global Risk & Regulatory Technology Practices, Infosys Financial Services Domain Consulting Group.

Anjani has over 20 years of comprehensive experience in IT, domain, and process consultancy. He manages several strategic initiatives including thought leadership publications, solution enablement support, research and competency development program, and marketing efforts from a domain perspective. He has authored large number of high-impact whitepapers and articles; including many that have been published on reputed external forums.

Amit Jayaram Lal

Lead Consultant, Regulatory Technology Practice, Infosys Financial Services Domain Consulting Group.

Amit has over 16 years of comprehensive experience in domain and IT consultancy. He has been part of several strategic Fraud and AML domain projects and key initiatives, including internal publications on emerging trends, and RFPs.

External Document © 2022 Infosys Limited

References

1. One Year after COVID-19, New TransUnion Research Shows Digital Fraud Attempts Against Businesses Have Increased by 46%, Mar. 23, 2021, newsroom.transunion.com.
2. PayPal Introduces New Fraud Protection Tool For Merchants, Apr. 12, 2021, pymnts.com.
3. Study: Banks See Rise in Fraud Attempts, Associated Costs in 2021, Jan. 6, 2022, bankingjournal.aba.com.
4. UEBA security solutions detect and respond to anomalous user behavior, logrhythm.com.
5. PayPal reveals 4.5 million accounts were 'illegitimate', shares plummet, Feb. 03, 2022, finextra.com.
6. Behavioral biometrics enhance digital security for insurers, Kim Brown, May 28, 2021, propertycasualty360.com.
7. TransUnion and Neuro-ID Partner to Help Insurance Industry Find New Ways to Support Customers, Improve CX and Detect Fraud, May 05, 2020, newsroom.transunion.com.
8. Behavioral biometrics reduce fraud losses for oft-targeted Zelle payments, Karen Hoffman, Jun. 01, 2022, scmagazine.com.
9. Entersekt partners with Capitec Bank to Boost Security and Reduce Friction for E-Commerce Transactions, May 10, 2022, businesswire.com.
10. Behavioral Analytics Fights eCommerce Fraud and Friction in Real Time, May 19, 2022, pymnts.com.
11. Fico acquires behavioral biometrics company to integrate AI-driven authentication, Luana Pascu, Nov. 11, 2019, biometricupdate.com.
12. TypingDNA introduces continuous biometric authentication for remote workers, Chris Burt, Jan. 20, 2022, biometricupdate.com.
13. Feedzai Acquires World's Most Advanced Biometric Platform, Revelock, Creating the World's Largest Financial Intelligence Network (FIN) to Secure Cashless Commerce, Aug. 04, 2021, globenewswire.com.
14. Adaptive fraud prevention with behavioral biometrics launched by Kount to stop account takeovers, Chris Burt, Mar. 17, 2020, biometricupdate.com.
15. LexisNexis Risk Solutions Buys BehavioSec for Behavioral Biometrics, May 04, 2022, pymnts.com.
16. BioCatch launches behavioral biometrics-based Age Analysis to protect elderly from fraud, Frank Hersey, Oct. 06, 2021, biometricupdate.com.
17. BioCatch's behavioral biometrics mule account detection patent approved, Alessandro Mascellino, Feb. 08, 2022, biometricupdate.com.
18. Mastercard Unveils Suite of Healthcare Solutions to Detect Fraud & Protect Health Data, Jasmine Pennic, Oct. 28, 2019, hitconsultant.net.
19. Mastercard taps biometrics and behavioral analytics in new product suite for healthcare partners, Chris Burt, Oct. 28, 2019, biometricupdate.com.
20. Ping Identity adds behavioral biometrics and bot detection with SecuredTouch acquisition, Chris Burt, Jun. 22, 2021, biometricupdate.com.
21. BlackBerry unveils enterprise behavioral biometrics, Featurespace adopted by NatWest, Alessandro Mascellino, Oct. 08, 2020, biometricupdate.com.
22. BlackBerry unveils enterprise behavioral biometrics, Featurespace adopted by NatWest, Alessandro Mascellino, Oct. 08, 2020, biometricupdate.com.
23. Aetna Adds Behavior-Based Security to Customer Application, Steven Norton, Jul. 18, 2017, gurucul.com.
24. Jack Henry helps banks and credit unions manage risk while optimizing the digital experience with NuData Security's behavioral technology, Jun. 30, 2020, nudatasecurity.com.
25. Featurespace Launches Automated Deep Behavioral Networks, Business Wire, Feb. 25, 2021, financialpost.com.
26. PYMNTS Intelligence: Leveraging Behavioral Analytics to Complement Other Fraud Prevention Measures, Apr. 29, 2022, pymnts.com.
27. Why Data Scientists Say Behavioral Analytics Is a Security Stack Must-Have, Apr. 27, 2022, pymnts.com.
28. BEHAVIORAL BIOMETRICS MARKET - GROWTH, TRENDS, COVID-19 IMPACT, AND FORECASTS (2022 - 2027), mordorintelligence.com.
29. Global User and Entity Behavior Analytics Market to Reach $4.2 Billion by 2026, Jun. 10, 2021, prnewswire.com.

For more information, contact askus@infosys.com

Infosys®
Navigate your next

© 2022 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.