[White Paper]

Next Generation Authentication Using Data Science

Authors

Mike Towers, Jim Routh, Shahrokh Shahidzadeh, Alan Krassowski, Dr. Abdulhrahman Kaitou

Table of Contents

Overview

For too long, enterprise leaders have been forced to choose between two extremes: authentication systems with scores of passwords across different components vs. allowing unfettered access using a single password for all systems resulting in poor security. To provide controlled access to systems with both greater security and less friction, the traditional password-based paradigm must be transcended. Digital authentication must be re-conceptualized beyond a simplistic “in” vs. “out” binary decision made in isolation. In this paper, the vision of Next Generation Authentication (NGA) as a more effective, multi-sensory, dynamic, risk-based authentication system is presented. NGA leverages technology advances in computing power and data processing that have been compounding for more than six decades. The main components for the NGA stream processing are introduced, highlighting a modern system architecture with streaming data at its core.

Introduction

Computer password systems have largely followed the original pattern of organization and operation since 1960. After a single password verification, the user is “in”; no subsequent authentication is applied throughout the user session. Yet over the last decade, password-based authentication has become increasingly troublesome. Users, overwhelmed with oft-forgotten passwords, now keep dozens of passwords stored on a file, or use a single sign-on (SSO) that caches multiple passwords behind yet another ultra-sensitive password, or derive similar passwords for a wide variety of different online systems. By creating new avenues of attack, they increase security risk for the enterprise. Meanwhile, attackers have adopted increasingly powerful new tools for social engineering, cracking passwords with brute force methods, and intercepting authentication protocols. As a result, billions of passwords are now available on the dark web. Traditional multi-factor authentication (MFA) attempted to strengthen security for passwords but created excessive friction for both users and system administrators. And attackers regularly exploit weaknesses in SSO and MFA implementations. The severity of this problem has been drawn into sharp relief with the unprecedented scale of SolarWinds and Microsoft Exchange attacks in 2020-2021, both of which included attackers bypassing MFA. Assume all passwords have been hacked--or soon will be--regardless of how intricately and uniquely they have been devised. Cybercriminals have easy access to over 3 billion harvested credentials from digital consumers worldwide. Biometrics can be reduced to a few binary traits; while a fingerprint or facial scan appear to be distinctive and safe, they too can be spoofed when they exist in digital form outside of special hardware. Two-factor authentication can impose time limits on users at every log-in, producing friction and fatigue. And temporary codes over insecure channels can be intercepted during transmission. Traditional multi-factor authentication (MFA) security solutions lack context and rely on too few attributes. Without a change in approach, all enterprise data can be compromised.

Authentication as a Continuum

This is why authentication is best conceptualized not as a single event with a binary yes or no, but rather a continuum. Next Generation Authentication (NGA) provides a simple way to access systems, while ensuring high security over time, throughout the life of each session. Unlike traditional authentication akin to a single guard at the front door, NGA is an embodiment of a cadre of digital guardians equipped with multiple security cameras and other sensors protecting all entry points. These defenders patrol the hallways, recording throughout the day and night. They are also empowered to respond and take appropriate actions including immediately ousting any would-be intruders. By harnessing the powerful new capabilities of behavioral modeling and modern data science, the dangers endemic to password-based authentication systems are alleviated while the digital experience for both end-users and system administrators is improved. This paper demonstrates techniques employed by NGA to efficiently collect data from several sources, order and make sense of the data, and store the enriched information for later reference. This can include for commonality analysis, when an intrusion is detected in one place to prevent similar future intrusions elsewhere.

Balancing Access (friction) vs. Control (who has access to what)

It is critical for CISOs to take an adversarial stance relative to every process and decision, with a full appreciation of the capabilities of contemporary threat actors. CISOs are challenged with protecting the attack surface of the enterprise as it evolves, as well as addressing the control requirements for emerging technology capabilities to support the business strategy and direction. Failure in these efforts has huge financial and public relations costs that can invite further regulatory and shareholder scrutiny. Time, attention and money are too often squandered attempting to defend against attackers with antiquated and inadequate defensive measures. Every CISO today needs to recognize the gradual obsolescence of passwords, especially because incident response data shows that stolen credentials are part of the threat vector of 90% of enterprise security incidents. NGA provides an alternative approach for CISOs that:

1) Improves security
2) Removes friction for the digital consumer/workforce
3) Results in lower operating costs for the enterprise
4) Better enables a trusted digital experience for all stakeholders

The first three of these benefits form a compelling case for investing in a strategic direction that reduces and eventually eliminates the dependence on passwords as the primary authentication control for the enterprise. Yet the benefits of improving the trusted digital experience, and a full accounting of the costs of not doing so, are often overlooked. In addition to protecting-what-they-know, CISOs must also securely-enable-the-new for the enterprise to remain competitive and thrive.

NGA Core Architecture Building Blocks

The NGA architecture rests on three main pillars:

1) Stream data acquisition and feature extraction
2) Training and deriving inference into and from AI/ML models
3) Making risk-based decisions to orchestrate effective actions that enforce policies, including a feedback loop to fine-tune the system

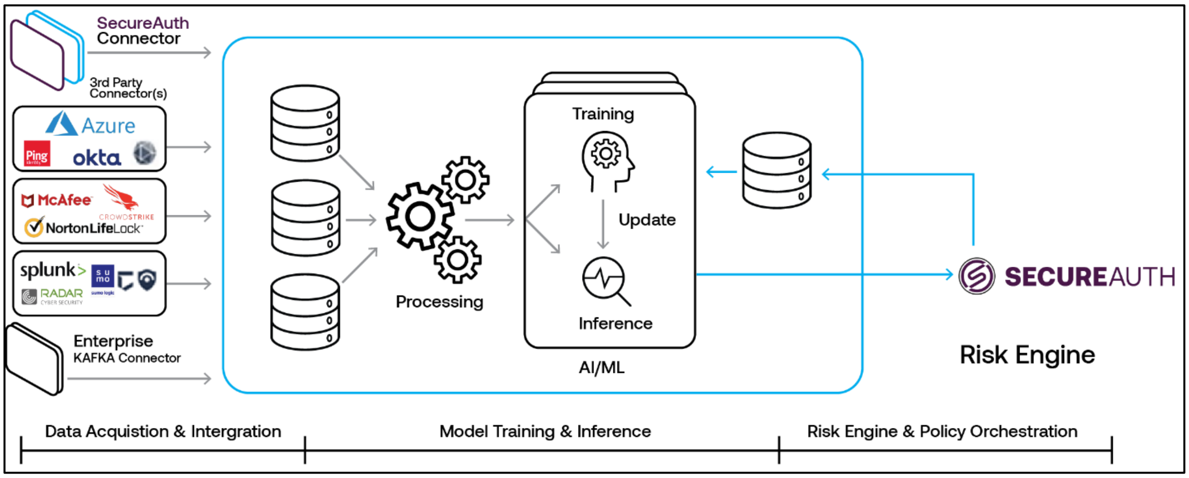

Figure 1: Next generation authentication system architecture

Data feeds from external systems (such as SIEM logs and APIs, DNS Security logs, Content Delivery Network (CDN) logs and APIs) flow through the data acquisition component. Data is then cleaned, and features are extracted into the Feature Store. The data integration component enhances and integrates data streams from several sources and unifies the data format. The internal data stream flows into the inference component of the AI models and back to the Model Store, along with labels acquired from inference, for later training and fine-tuning of the AI model.

Both batch and stream processing are employed within the NGA architecture. For example, the AI model management includes both an incremental training of some AI models as well as batch training. When processing streams, data is processed as it becomes available, resulting in a fast response to changes. Stream windows can overlap and have complex forms that are hard to orchestrate and schedule in systems limited to traditional batch processing. In this way, the rich and robust stream processing capabilities of NGA enable continuous authentication by being able to monitor user actions in near real-time and quickly detect and intelligently respond to anomalous behaviors.

The incremental training allows the latest data to contribute to the inference decisions. However, because this also tends to decrease model accuracy over time, the accuracy is periodically readjusted with batch training on a freshly comprehensive dataset.

All of the prior data processing and inference from AI models then flows into the Risk Engine. The Risk Engine provides actionable intelligence by determining a dynamic level of assurance (DLOA) score for observed user actions.

Continuous Actionable Intelligence

The NGA architecture can be considered as analogous to parts of a mammalian brain. The acquisition and storage of data in NGA is similar to a digital hippocampus, remembering novel patterns and events that can identify and distinguish individuals from each other. The AI models that can be used to predict behaviors as being normal vs. anomalous are similar to a digital cerebellum.

The Risk Engine is like a digital neocortex, combining the perceptions from all of the sensors, and providing a rational basis for taking insightful actions based on reasoning, inference, rules and past learnings. Similar to how the motor cortex transforms multisensory information into motor commands, with policy orchestration, the enterprise can specify appropriate responses and enforce actions related to observed behaviors in relation to events deemed significant.

All enterprises have their own unique DNA and the equivalent of a nervous system for communicating among stakeholders. An NGA deployment does not need to replace existing enterprise policy orchestration tooling. However, NGA can significantly complement and enhance one of the most vital parts of policy enforcement - namely, getting a solid level of assurance about who the enterprise is encountering in a given interaction. What is the probability this is an employee vs. intruder? To what degree does this look like a customer vs. an attacker? Anticipating and quickly making accurate determinations to appropriately respond is the core value proposition of NGA.

Studies show that 60-80% of the energy of the human brain is used for making predictions. If humans had to observe, detect, recognize, and classify every scene from scratch, they would have never survived. They would be unable to protect themselves or prevent harm from coming their way. And yet, many enterprises have been approaching authentication without the powerful and intelligent predictive analytics available in NGA. As the online environment becomes more dangerous and unforgiving, continuous authentication based on predictive analytics is fast becoming a necessary evolutionary survival adaptation. Said another way, outsmarting sentient opponents seeking to harm the enterprise requires up-leveling the enterprise’s intelligence and digital nervous system.

Benefits of NGA

NGA enforces the behavioral verification, which can then detect imposters with stolen user credentials inside the system or bad behavior of previously legitimate users who have since gone rogue. This is the core differentiator of NGA: permitting digital behavioral modeling of users, classification of actors (threat actors vs. legitimate) and a path to anomaly detection and commonality analysis. Combined with an adaptive, dynamic, flexible architecture for processing both existing and new data streams for the purpose of risk mitigation, this allows for adaptation in the face of ever-evolving new threats.

The ability to measure the efficacy of security controls over time as the threat surface changes is a key driver to adopt NGA. Measuring well is not only necessary for effective management, but it also helps the enterprise identify and remove technical debt stemming from older security controls with subpar (or even negative) ROI. A key benefit of NGA includes the agility of being able to swap out underperforming risk models for more effective ones in the face of an ever-shifting threat landscape. NGA can also help leverage more value from data lakes fed by existing enterprise security controls.

Behavioral verification is continuously verified authentication over time after every user action of interest. These user actions can be the user’s calls to a set of services in the system. In a microservice architecture, every functionality in the system is modeled with a microservice, and each microservice typically records logs for every call. Similarly, the trend towards composing systems via REST APIs with discrete functionality on well-defined interfaces also assists in being able to track significant events. In this way, modern cloud-based SaaS design contributes to behavioral verification’s feasibility and efficacy.

The NGA approach is based on a simple AI and machine learning fundamental. Every event can be represented in mathematical terms. A sequence of events of interest representing a repeating pattern can also be represented mathematically. A comparison of the two results in a deviation score that measures the alignment to the pattern or deviation of the pattern. Deviation of the pattern represented with a number can be used to establish a threshold (a specific number or range requiring action) and thresholds can trigger orchestration (workflow). This data science fundamental (often referred to as cluster analysis) forms the foundation for continuous behavioral-based authentication enabled by a streaming data architecture.

Since this is all based on mathematical formulas or algorithms, all of the calculations can be done in close to real-time. Humans can adjust the threshold scores whenever they wish based on data analysis while the system continues to operate.

The discovery of digital identities based on pattern matching in real-time is a use case without overwhelming complexity. Alignment of treatment with a specific score as a result is also straight-forward. Determining behaviors that deviate from a pattern across multiple attributes is a clear indication of a threat actor gaining unauthorized access to a system. Using AI to identify threat actor behavioral patterns is much more challenging for the simple reason that threat actors adjust and adapt their behaviors to discover control weaknesses to exploit. Determining if an online user's attributes align to a known-good pattern is much less challenging. The more attributes used, the better the results. The more data used, the better the results and the fewer the false negatives. Actual implementation experience suggests that threat actors face much too much friction in this model to attempt to replicate behavior across multiple attributes, so they give up. The same experience suggests that there may be cases where a step-up or additive authentication control is applied when it may not be necessary, but this is much rarer than in previous solutions (about 0.002% of the time).

Much of the discussion to date about AI applied to cyber security controls involves the identification of the threat actor using deep learning and machine learning algorithms applied to the discovery of threat actors. It's imperative for the CISO to instead focus on applying continuous behavioral attributes of the legitimate user/customer to determine if the behavior matches the identity being represented. The outcome will identify the threat actor based on the deviation score. This is much easier than attempting to find the threat actor through data analysis. The NGA approach works well in practice because establishing patterns from multiple attributes to confirm identity using continuous behavioral based authentication does not require advanced data science or scientists.

Updating AI models in traditional systems occurs, optimistically, every 24 hours. NGA is designed to perform an incremental update to the AI models over a defined stream window, which makes detection of imposters possible at a low latency. This provides clear visibility and high transparency of user activities in the system, including the rapid interception of intruders, before they can do the most damage. Stepping up authentication prior to potentially risky actions, post-authorization, can sometimes mean the difference between a successful attack vs. a thwarted attacker.

As SolarWinds and Microsoft Exchange hacks in 2020/2021 have shown, many enterprise leaders were shocked because they had been under the false impression that their systems were not compromised. While the 'assume breach' stance is useful, learning about significant system compromises several months after they occurred is a painful and humbling ordeal, better avoided than experienced. Data mining in the NGA architecture can help determine whether a prior system compromise by attackers is still in effect, and close it down swiftly.

The NGA architecture provides both built-in cross-organizational intelligence, as well as a framework for plugging in 3rd-party risk analyzers. This allows an enterprise to take advantage of cross-enterprise learnings based on real-world experiences of other organizations successfully fending off attackers. Like the collective intelligence across multiple antivirus vendors in the antimalware space has enabled the industry to better identify malware vs. benign executables, the sharing of risk models/algorithms across organizations through NGA can provide a form of herd immunity against malicious threat actors among inoculated enterprises.

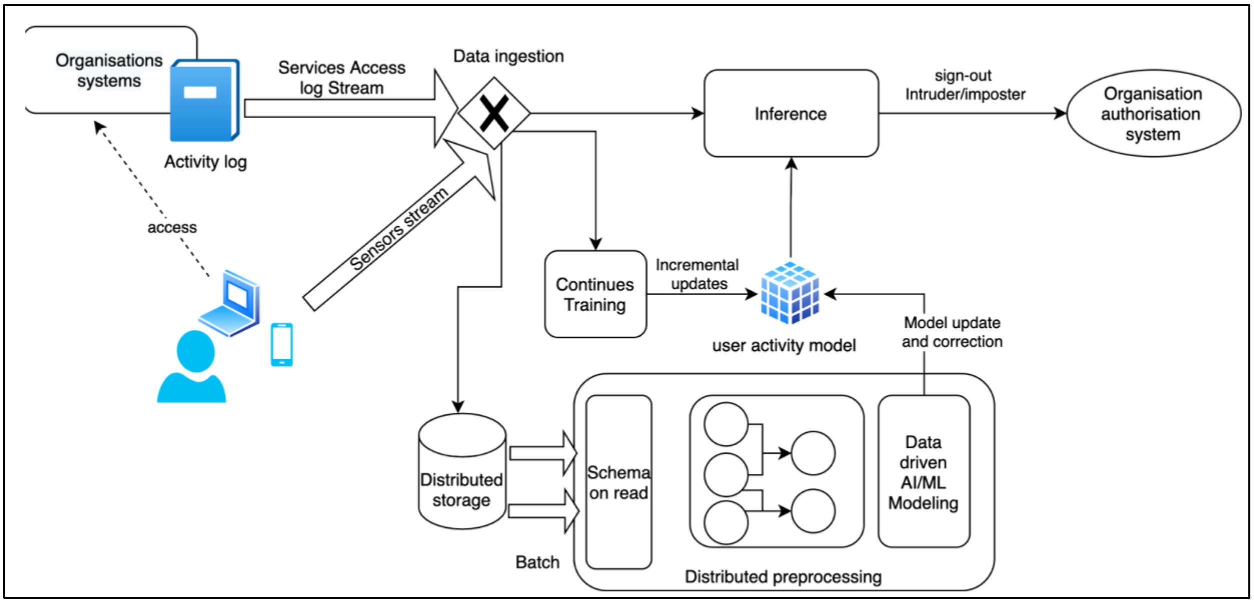

Figure 2: Next generation authentication system architecture

NGA advantages over current legacy approaches

Besides the high performance, elevated security, lower cost and less friction, the next-generation authentication system affords the following key advantages:

- Behavioral authentication
- Infrastructure for highly secured passwordless systems
- Transparency of the user activities in the system; user activity is directly monitored by the NGA system, data analysts, and IT managers
- Rapid interception of intruders
- Marking all the infected services by the intruder throughout the session

Behavioral Authentication

Humans constantly assess their environment and base their decisions on their observations and prior experience. In contrast, most existing security solutions neglect contextual information and are static in nature, never adapting to new situations and challenges. Without an element of time, context is yet another binary indicator. Hence, throughout this paper, the importance of context and also behavior is highlighted, the latter of which is derived from context yet additionally has an element of frequency and time order.

By constantly observing and analyzing users' routines, biobehavioral® modeling creates discrete models that can predict the next actions of users and detect and distinguish legitimate, suspicious, sub-optimal and even dangerous behavior. This modeling process applies AI and machine learning technologies on data streams. From browser behavior and computing devices to more subtle patterns, unique combinations of factors unambiguously characterize users and allow the SecureAuth risk engine to rate behavior. Consequently, it computes a dynamic level of assurance that takes the maximum amount of relevant contextual information into account. Similar to the dynamic nature of human life, bio-behavior continually observes and adapts to changes. In this way, an NGA deployment learns and grows with its users, representing the heart of continuous behavioral authentication.

Privacy Issues and Ethical Concerns of NGA

Collecting and analyzing data with algorithms naturally raises a variety of privacy and ethical concerns. It is common for CISOs to constantly wrestle with privacy and ethical boundaries as they seek to put greater protections in place to secure the enterprise environment from attackers. Failure to strike the right balance can result in public relations challenges and a reduction of trust in the enterprise and its leaders.

In 2018, when Alex Stamos left his role as Chief Security Officer of Facebook, he wrote an internal memo containing some thought-provoking comments worthy of consideration:

- “We need to build a user experience that conveys honesty and respect” “We need to intentionally not collect data where possible, and to keep it only as long as we are using it to serve people”
- “We need to listen to people (including internally) when they tell us a feature is creepy”

To avoid being perceived as overly watchful, user behavior tracking needs to be considered in the correct context and managed with appropriate principles, guardrails, and governance.

In general, categorizing different contributors to privacy and ethical risk can also be helpful for framing an exploration of these issues:

1. What type of data is used? (e.g. internal to the company vs. external/personal/public)
2. How is the data used? (reactive vs. proactive/predictive, to secure the enterprise environment vs. sell the data to others)
3. Who can analyze the data? (automation/machines vs. humans)
4. Who makes decisions based on the data? (independent 3rd-party vs. various workforce staff in various functions)
5. What is the level of aggregation of data? (anonymized, aggregated, or individually identifiable information)

More specifically, achieving acceptable levels of cybersecurity vigilance has always required a certain level of data collection and processing. Today, the modern use of behavioral data in authentication for the purposes of security and fraud prevention is aligned with the evolution of global and local privacy regulations (GDPR, CPPA, etc.). And there are clear precedents for using behavioral data to improve the digital experience for digital consumers and employees that are also aligned with the recent evolution of privacy regulations globally.

Organizations that have implemented an NGA architecture have made specific design decisions based on their preference for managing the privacy of digital consumer behavior:

1. Behavioral attributes are selected when they are benign to exposure and the selection process is validated by privacy professionals.
2. The attribute data is never stored--it is converted in the system to an algorithm and the risk engine uses algorithms exclusively.

3. Biometrics should be considered distinct from behavioral modeling. Given their sensitive nature, the use of biometrics should be left on edge devices, protected by modern operating systems within secured hardware--and not centrally collected or processed in the cloud.

These three design principles, recommended by SecureAuth, are foundational for the use of an NGA architecture to protect user data privacy today and well into the future for the enterprise and are based on specific enterprises that have implemented NGA successfully.

By implementing an effective form of authentication that can accurately distinguish between legitimate users vs. attackers, NGA not only serves the needs of the enterprise, but also provides users the benefits that privacy proponents advocate for. For example, in her book, The Age of Surveillance Capitalism, Harvard Business School professor Shoshana Zuboff argues that every user has a “right to sanctuary” within the context of their online experiences. Those who agree with this right in principle must also recognize that, in practical terms, no user can take refuge in safety when attackers are also allowed to freely enter the environment and cause mayhem. A secure environment is a necessary precondition for the sanctuary, and a large part of every CISO’s job is ensuring that safe space.

The SecureAuth NGA platform is also categorically different from what Zuboff calls a ‘Big Other’ like Facebook. In NGA, no behavioral data is sold for marketing purposes nor used for any purposes other than authentication. The NGA architecture does not “shape human behavior for others’ ends”, as Zuboff dubs an Instrumentation tool. Instead, NGA empowers both the enterprise and the end-user by providing an improved environment for safely negotiating their interactions with each other in the online world.

After all, the creation of a relatively safe space for interaction among legitimate actors is fundamental to a productive business environment. This necessarily requires analysis and synthesis of data about both the participants and the environment for a wise, risk-based stewardship of the environment. The NGA approach preserves each user’s unique sovereignty. It keeps users safe from identity thieves and impersonators who might otherwise sully their reputations as good actors while also preventing damage to the shared common space among participants. By contrast, the failures of password-based systems in these efforts have become intolerably unfair to all legitimate actors. With appropriate principles, guardrails and governance in place, NGA fixes an imbalance in the ecosystem by empowering users to assert their legitimacy by simply presenting themselves as they are to the system, instead of struggling to contort themselves around the limitations of the rapidly obsolescing password-based paradigm.

SecureAuth models digital behaviors of good actors vs. potential threat actors in order to detect fraudsters. The behaviors of legitimate users are derived from their application habits, devices, browsers and networking context. This enables a set of unique risk analyzers that feed to SecureAuth’s risk engine for determining the authenticity of a claimed identity when it is presented to the enterprise.

SecureAuth does not use behavioral biometrics such as typing speed, how a user swipes or holds a phone. First and foremost, they are not reliable indicators. People alter such behaviors to suit their environment and their own physical and mental states. Holding a glass of water, ingesting varying amounts of caffeine, juggling a toddler on one’s lap, walking the dog, sitting vs. standing at a desk, etc. can all cause dissimilar behaviors at unpredictable times. Second, the line between people’s personal and work lives has become increasingly blurred. Because of this, enterprises have found that the false positive rates of behavioral biometrics have become unacceptably high. Third, behavioral biometrics are also prone to replay attacks via synthesized machine generated behavior.

Analytics from behavioral biometrics is also concerning for users. Private medical conditions, such as a sensor detecting a shaking phone that corresponds to a tremor in the hand holding it, have no legitimate business being analyzed when negotiating an enterprise session logon. Similarly, a phone detecting that the user is walking with a limp should not be perceived as a basis for increasing health insurance fees. Such derived physical attributes may also be in conflict with GDPR and other privacy guidelines such as CPPA.

Exponentially far away from behavioral biometrics, SecureAuth's digital behavioral modeling to prevent fraud is aligned with GDPR Recital 47.

Use Cases

The primary use case for biobehavioral® authentication involves an end-user attempting to access either a remote or local resource that requires authentication. While device fingerprinting (for remote) and biometrics (for local access) can be used for authentication, both are vulnerable to replay attacks. Multi-factor authentication (MFA) that requires an additional out-of-band device (e.g., a confirmation on a mobile phone) significantly increases security. However, this solution is insufficient, as a loss of the device and the increase in friction is significant.

The biobehavioral® approach also relies on an out-of-band device such as a mobile phone or wearable device, but offers three important advantages:

Event Sequence Modeling and Early Warning: Stochastic approaches are typically well suited for smaller data sets, establishing a model after a small number of days of observation, scaling well to extend to daily, weekly and monthly models. The spatiotemporal modeling employs a variant of Gaussian mixture models. From the general formula it can be seen that the model represents a probability density function that is composed of weighted normal distributions. The normal distributions represent cluster coordinates at times that belong to the same logical location. One cluster might be a user's workplace with a 50m radius around its entrance associated with a time interval from 7am to 5pm. Graphing other activities inclusive of location signals, such as using derived data from badging into a controlled location as well as ambient intelligence derived from spatiotemporal and geostatistical data, can also help with event sequencing and calculating risk.

1. Authentication factor: The system benefits from the rich sensors in modern mobile devices. Based on that, the employed artificial intelligence uses machine learning (AI/ML) to create models that can:
   a) Detect regular and abnormal behavior,
   b) Recognize anomalies, e.g., spatial temporal, in the ambient sensor data and,
   c) In general, verify whether it is still in the possession of its owner.

As such mobile devices are an essential part of the authentication process. It provides additional, reliable information such as the owner's verified location and current activity. For instance, a banking transaction may be unlikely if the user is currently outdoors exercising--and even more so if the transaction is requested from a desktop computer. On the other hand, the system is adaptive, and behavior considered unusual by a majority can be perfectly normal for an individual's unique biobehavioral® model. Eventually, the models contribute to the overall level of assurance in an access that grants reduced friction to the end user.

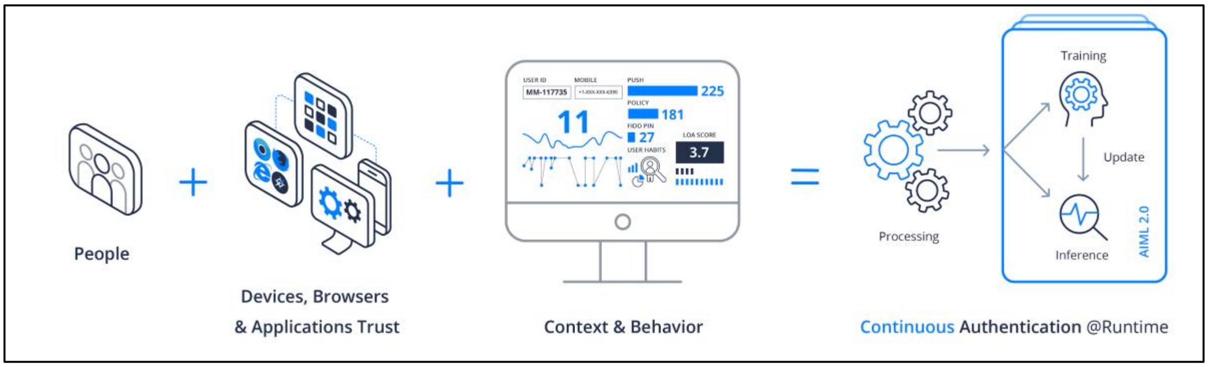

Figure 3: Continuous Authentication at Runtime

2. Biobehavioral® as the determining authentication: In addition, the system can play a more active role in the authentication process. Access from a verified system can be allowed with minimal friction. In this situation, Biobehavioral® becomes the determining authentication factor.
3. Prediction of user behavior: The machine learning models used in NGA capture an abstract representation of user routines and unique characteristics on varying time scales. Similar to how the human brain spends 60-80% of its energy on prediction, the variants applied in the biobehavioral® system of NGA are capable of predicting future behavior, activities and locations. As such, NGA can preemptively act on conditions (similar to smart mapping services can suggest traffic avoidance patterns) or prepare a resource ahead of time.

   Possible fields of application among others are:
   a) All flavors of access to online resources such as banking, online shopping or remote login
   b) Securing mobile payment and
   c) Physical Access Control Systems (PACS)

Note that derived solutions of the same base behavioral modeling system can be used for applications other than authentication including both anomaly detection as well as corrective behavior systems using mobile and ambient sensors.

Operational Challenges and KPIs

Improving the digital consumer experience for B2C enterprises results in higher margins from higher consumer retention and an increase in digital consumer activity. Given the bottom-line, implications for the enterprise, CISOs need to consider how best to measure the key performance indicators related to lower customer attrition and a higher concentration of digital activity based on the reduction of consumer friction for the enterprise. Research confirms that reducing digital consumer friction improves the digital consumer experience resulting in more active consumers using the features of the digital assets. Digital marketing resources have established measurements for digital activities that can and should be used for determining the right KPIs for the NGA program for each enterprise.

Enterprises must manage three main considerations when it comes to cybersecurity: vulnerability, friction, and cost. Vulnerability increases when utilizing insecure binary authentication methods, while friction accrues as the use of these methods become overbearing and inconvenient. Accumulating costs come with both vulnerability and friction: the cost of deploying and maintaining authentication solutions, of help desk, of breached data, of multi-vendor non-unified solutions, and of lost productivity due to authentication troubles. The unfortunate truth is that the efficacy of controls deteriorates over time. Therefore, a technology that treats authentication as a continuum, instead of a binary event, is critical in defending against threat actors' increasingly advanced tactics. This is the only way to maintain the delicate balance between the two competing objectives of IT Operations: service level-speed and secure access management.

Moreover, organizations which have the challenge of dealing with both internal Identity Access Management (IAM) and external Consumer Identity Access Management CIAM) often have a bifurcated security stack that adds to the cost and complexity of security operations. Next Generation Authentication provides a common platform serving both IAM and CIAM by consolidating the core building blocks including the risk engine, policy orchestration, smart data hub, and device and browser trust modules.

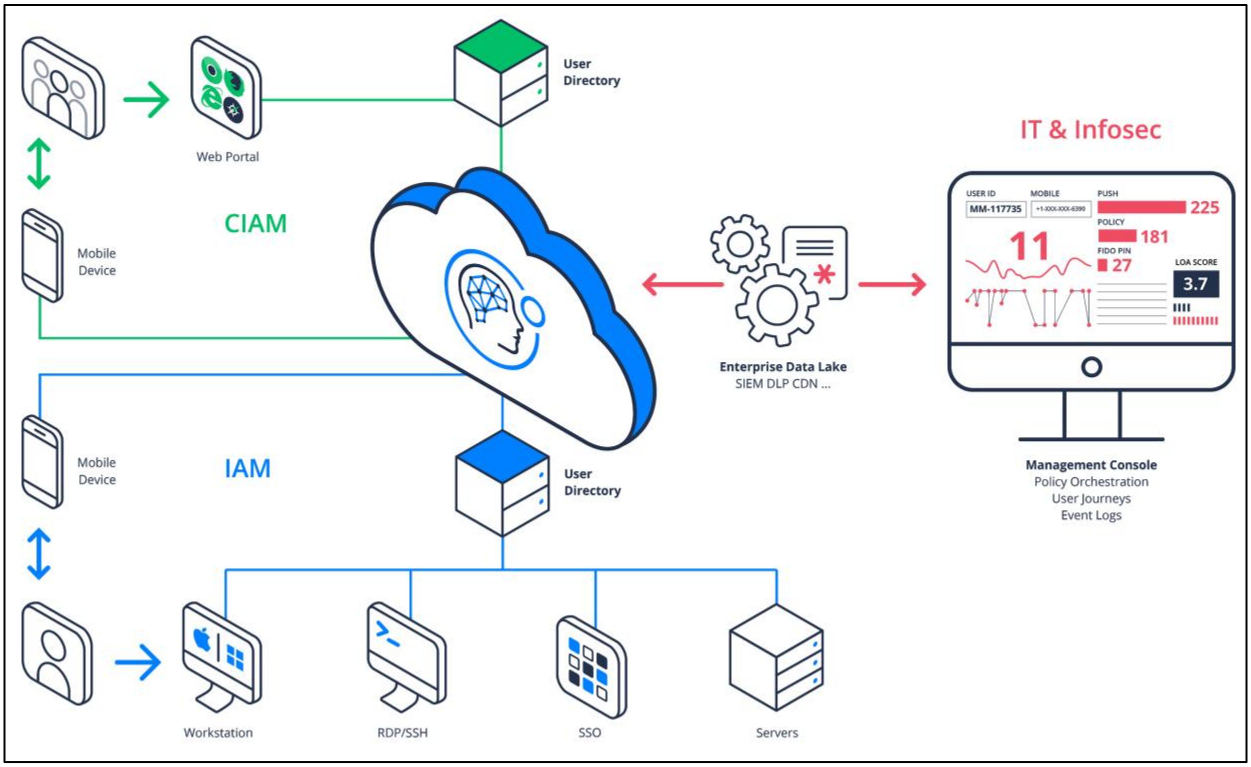

Figure 4: NGA's Consolidated IAM-CIAM Continuous Authentication Platform

Key Performance Indicators (KPIs) are essential for the enterprise and the CISO to manage stakeholder expectations for the change in digital consumer behavior. Digitally savvy consumers today are conditioned to seek self-help options that may be more responsive and meet their needs. Larger segments of digital consumers rely on conventional forms of support such as calling the help desk. Reductions in digital consumer friction directly reduces the need for help desk calls by consumers when passwords fail. The cost of calls in a consumer help desk function for enterprises are easily calculated and tracked in enterprises and are typically measured in the cost per call and the average time per call. Eliminating the infrastructure to support automated and manual password resets results in millions of dollars of savings annually going forward. This is a big part of the business case for the NGA initiative.

The reduction in digital account takeover is the third area of the NGA business case that needs focus from the CISO. Enterprises have been measuring the cost and impact of using credentials for authentication purposes for many years. The elimination of the need for credentials creates a state for the enterprise that is unusual: no more account takeover. This phenomenon is unique for the enterprise using NGA in that there is no historical data in recent decades where account takeover was eliminated. The facts are that those enterprises that implemented NGA eliminated account takeovers.

The assume-breach principle can also be applied to the continuous behavioral based authentication architecture itself. For example, suppose the risk engine was hacked by threat actors. In that case, no attribute information is available, only number strings that are meaningless to the attacker. Similarly, threat actors cannot use behavioral replay attacks to bypass authentication controls since there are too many attributes in synthesize in real time, and other replay attack preventions are in place. As a result, threat actors will focus their energy on those enterprises using passwords where their risk/reward is greater and the success rate is higher.

Enterprises can and will have situations of false positives using an NGA architecture, where some behavioral attributes deviate from the pattern enough to trigger a step-up authentication control. In one enterprise that implemented continuous behavioral risk-based authentication, the actual number of false positives was 0.002%. Improving models can and will reduce the false positive rate over time.

In the coming years, end-users will delight in being able to rid themselves of the hassles of passwords. Yet transition periods require learning about and adopting new habits, which can create temporary hurdles to overcome. Accurately measuring the overall happiness or satisfaction of customers with objectively quantifiable scores can prove tricky.

Some enterprises use the Net Promoter Score®, or NPS®, as a metric for measuring how well they are performing in terms of customer experience (CX). NPS seeks to measure the likelihood of customers recommending the brand to a friend or colleague. In such environments, statistically significant changes in NPS from before and after the deployment of NGA can be used as one indicator about the effectiveness of NGA relative to the overall perception of the enterprise's brand. Because NPS will be measuring a significant change in the user authentication journey, applying NPS effectively to NGA needs to be considered within the scope of the enterprise's customer experience management program. And since NPS measures user perceptions, the way that the new authentication experience is designed and communicated to end-users is at least as important as how well the underlying technology is performing its security function.

The same is true for enterprises that use NPS or similar surveys internally to gauge the satisfaction of their own workforce in the context of an IAM deployment of NGA. In both cases, involving enterprise User Experience (UX) designers and corporate communication staff in the NGA roll-out process will produce optimal results. One of the most significant challenges for the CISO introducing an NGA architecture design is to encourage talented architects to consider authentication as a continuous process vs. an event with a binary outcome. It means un-learning what was taught when the workforce was first exposed to IT and the authentication process. Moving from a single event to a continuous process can be difficult for skilled IT practitioners to adjust to. The CISO needs to recognize that the NGA architecture represents an evolution in identity access management. Combined with the traditional role-based access control (RBAC), it enables behavioral-based access controls that takes advantage of underlying streaming data architectures. The CISO should also anticipate months of time for an enterprise to consider the possibilities of the NGA architecture. When there is no precedent for a technology like NGA, it is more difficult for the CISO to engage and influence IT practitioners to consider the necessity and benefits of continuous authentication. The most compelling rationale for the NGA approach is the growing obsolescence of passwords forcing smart people to consider changing the well-established paradigm of event-driven authentication.

There are several sources of resistance to a continuous behavioral based authentication model within an enterprise that are common based on previous implementation experience including:

1. Technical platform gurus who worry that a new technology platform and paradigm may increase job security for them given their in-depth knowledge and expertise with the older technology platform
2. Technical architects and policy-oriented professionals who point out that current regulations support the use of passwords so perhaps the obsolescence of passwords is not well founded
3. Digital consumers who fall into two small segments:
    a) Those who grew up online with passwords and believe that their removal may represent less security largely because enterprises have always added friction with security features in the past. Therefore, they believe that removing friction must mean a lower level of security for the consumer.
    b) Those who understand the notion of capturing behavioral attributes for authentication but suspect the enterprise may consider using these attributes for purposes other than authentication (e.g., perhaps using attributes to determine health indicators and using this information to underwrite either a life or health insurance policy with fluctuating premiums based on interpreting the attributes)

In the first case, this is not a new phenomenon and is typical for any type of technology upgrade from an existing platform with a lot of legacy in an enterprise. The facts typically indicate that the replacement technology platform generally provides more marketability for the technology professional once the replacement platform is recognized as a substantial improvement.

In the second case, the current facts are that regulations are NOT requiring better authentication without using credentials. What is clear is that the growth of credential stuffing is causing the gradual erosion of authentication quality for the enterprise. For example, at the time of this writing, there are approximately 250,000 instances of a YouTube video produced to teach people how to use the Sentry MBA tool that is commonly used by threat actors to perform credential stuffing. If there are that many videos for training purposes, then there are likely hundreds of thousands or millions of viewers learning how to use a credential stuffing platform effectively. Some of those viewers are undoubtedly security researchers and system defenders. But a large percentage of attackers are being trained every day in how to subvert authentication systems using powerful tooling. Enterprise leaders cannot afford to wait for regulators to catch up with the offensive technologies of attackers.

The third example is specific to digital consumers based on previous implementation experience. A segment of the digital consumers has been conditioned to expect added security with friction for the consumer (remembering a password) and when the password is eliminated, they naturally believe that security is less effective. Some enterprises when faced with this resistance simply offer them the choice of keeping their passwords and logging in with them. The continuous behavioral based authentication is still applied in addition to the login credentials. Then there is another segment of users that understand the use of behavioral attributes and understand the benefits for authentication, but their technical savvy makes them question what the other use cases are outside of authentication that may be a possibility for the enterprise to use. A best practice in this potential case of resistance is to adjust the stakeholder communication plan to make it explicit that the behavioral attributes are used exclusively for authentication, the attributes were selected because they are benign and encrypted for protection.

Resistance to transformative change is common within all enterprises and should be both expected and addressed openly to help the enterprise come to the right implementation decisions using an NGA architecture.

The Journey to Next-Generation Authentication

In the multi-decade co-evolution with attackers, NGA has emerged as a better, faster, stronger, and revolutionary new authentication technology that defenders can employ to reclaim the upper hand. This is the desired destination for enterprises to steer towards.

As with any adventure, there are potential pitfalls. Some entrenched authentication vendors are now calling their solutions “passwordless” or even boldly assert that their solution is “true passwordless”, when upon further inspection, all they offer is a new way to mask passwords from the consumer or workforce. While reducing reliance on passwords is a step in the right direction, SecureAuth is the only platform today that gives an enterprise a fully integrated, evergreen platform for NGA.

Developing an implementation strategy for taking incremental steps towards NGA is certainly feasible and often recommended. New functionality can be phased in as appropriate to the enterprise needs. This is not an all-or-nothing proposition. SecureAuth’s NGA platform can be introduced to customers first, or the workforce first, and provides the same core platform to serve both CIAM and IAM needs in the same deployment.

When instantiating the NGA architecture, multiple deployment strategies can be accommodated. Deployments can be on-premise, in the enterprise’s own cloud or in SecureAuth’s cloud. Varying degrees of uptime and disaster recovery agility can be chosen, depending on preferences and budget.

In working with various organizations, SecureAuth has helped develop an NGA Manifesto that clearly outlines the specific reasons why NGA is imperative and how NGA can help the enterprise achieve its goals. Circulating such a document inside the enterprise helps provide clarity and a sense of mission. A manifesto can help align enterprise leaders to a singular vision, build consensus about the implementation plan, and wisely structure a roadmap with clear objectives and KPIs. Phased POCs can be designed to help the enterprise prove out value, provide proof-points and generally proceed in logical steps toward their next-generation authentication objectives.

The NGA approach has become possible through a confluence of recent technological advances. Stream-based processing on high-throughput, low-latency, real-time data feeds became enabled by cloud computing advances and sophisticated open-source software stacks. The steep rise and ubiquity of mobile phones has enabled multiple phone-as-factor options. As many enterprises have transitioned to Big Data / Data Lake platforms, those can now be leveraged to provide higher levels of insights and inferences using modern data science techniques.

With this breakthrough in security well-balanced with usability, trust itself can also become a visible asset for the enterprise, paying dividends with customers, partners, analysts, investors and the workforce. As the trustworthiness of the digital experience increases, the enterprise becomes more attractive to new prospects and investors.

It’s now time for **CISOs, CIOs, and CEOs to recognize this compelling case** and steer the enterprise in the right direction for the future. The technology maturity has arrived, and several leading enterprises have already made the commitment and implemented a continuous behavioral-based authentication model.

At its core, NGA performs five essential functions: Detect, Recognize, Classify, Protect, and Adapt. As a result, NGA enhances the digital experience for customers, partners, and the workforce while serving diverse needs of various stakeholders charged with protecting the enterprise. CISOs, as well as leaders in IT Operations, Risk Management, and Fraud Prevention will immediately recognize the security and user experience benefits of NGA. Furthermore, because NGA demonstrably reduces operating costs while protecting intangible assets, including the reputation of the firm's brand name and good standing within the wider community, CEOs and their CFOs will also grasp the value of the NGA approach.

About SecureAuth

SecureAuth is a leading next-gen access management and authentication company that enables the most secure and passwordless, continuous authentication experience for employees, partners, and customers. SecureAuth leverages adaptive risk analytics, using hundreds of human variables to create each user's unique digital DNA. This enables real-time continuous authentication and provides the highest level of security throughout the digital journey. Arculix by SecureAuth is the only platform that can be used as your single authentication solution or with your existing IDaaS/IDP. Our solution is deployable across hybrid and multi-cloud environments, delivering a truly passwordless experience to everyone, everywhere.