Smart Analytics
Solution Brief

Nok Nok Smart Analytics
Making Authentication Metrics Actionable

Measurement to Success

Most of us have likely heard the maxim "You can't manage what you don't measure[1]". This is sometimes attributed to Peter Drucker and sometimes to Lord Kelvin - we leave that to the historians. In 2012, Enisa published a paper on Return on Security Investment[2] (RoSI) and Gartner recently called out "Outcome Driven Metrics" as one of the Top 9 Trends in Cybersecurity for 20243.

Starting from a very high level, Global cybersecurity spend has increased from $36.6 billion in 2018 to an estimated $84 billion in 2024[5], which is a multiple of 2.7x. On the other hand, global cybersecurity fraud has increased from $0.86 trillion in 2018 to an estimated $9.22 trillion in 2024[4], resulting in more than a 10x multiple. Clearly, the costs resulting from fraud heavily outpace the amount the industry as a whole spends on prevention/cybersecurity. In other words, with our current approach, we, the industry, are not keeping up with cybersecurity fraud. We either need to spend a lot more, or we need to get smarter with our cybersecurity investments. Focusing on our current cybersecurity investments will require two strategies:

1. The cybersecurity industry needs to focus on robust security methods that treat the problem as opposed to "band-aids" that address symptoms.
2. Individual organizations need to optimize their specific cybersecurity/resilience approaches and tools.

Highlights

- Actionable Insights Through Industry Benchmarks
- Data Visualization for Stakeholders
- Fine-Grained Performance Measurement
- Enhances User Experience
- Streamlines Successful Deployment

On a positive note, with the availability of scalable phishing-resistant authentication (FIDO/passkeys), the industry has taken an initial step towards adopting robust security methods. More steps towards the "ePromiseland" are on the way[6] [7], that address the underlying problems of current cybersecurity approaches. What remains is for organizations to optimize their specific cybersecurity approaches and tools.

In order to optimize cybersecurity approaches and tools, it is important to (i) identify which metrics are more relevant and (ii) how to implement the findings from these measurements.

Determining Relevant Metrics

Capturing metrics is essential for several reasons. First, metrics provide quantifiable data that helps in assessing performance, identifying trends, and making informed decisions. They offer a clear picture of what is working well and what needs improvement, enabling organizations to optimize processes and allocate resources more effectively. Additionally, metrics foster accountability and transparency, as they allow teams to track progress against goals and objectives. Organizations can quickly identify and address issues by regularly monitoring metrics, ensuring continuous improvement and sustained success. Overall, metrics are invaluable tools for driving strategic planning and achieving long-term goals.

Success rate, time on task, and user error rate are seen as the most relevant metrics for user experience[8].

Utilization Rate

The **utilization rate** is often used as an indicator of project success. It shows what percentage of authentication events are performed using a method like passkeys compared to passwords or other methods.

Registration Rate

The registration rate represents the percentage of authenticator registrations attempted using the selected authenticator type compared to the total number of registered authenticators. Users need to create a passkey (i.e. register the related authenticator) before it can be used. This rate is a precondition for increasing the passkey utilization rate.

Registration Success Rate

Users need to create a passkey (register an authenticator) before they can use it for authentication. So, in order to increase the passkey utilization rate, you want a high registration success rate - ideally close to 100%.

Authentication Success Rate

Authentication is the front door to today's electronic services. If it is difficult to open, users get frustrated. Instead, you want to delight users with a smooth yet secure experience. When using legacy authentication methods such as passwords or OTPs, the success rate is low due to factors such as users forgetting their passwords, OTPs that users never receive, and more.

Fraud

A very obvious metric in cybersecurity is fraud, as it directly generates direct and indirect costs. The number of fraudulent events is easier for companies to measure. That needs to be multiplied by the average fraud cost per incident. Various stats are available (IBM cost of a data breach[10], Ponemon cost of authentication failure[11], LexisNexis true cost of fraud[12]), but it is important to understand the difference between customer fraud and workforce fraud.

However, measuring the number of fraudulent attempts still requires manual effort to verify whether incidents flagged as potentially fraudulent are, in fact, fraudulent or just false positives.

Authentication Time

Authentication is not what users *want* to do. Users just want to use a service, but your technology requires them to authenticate first.

This "distraction" should be short and not create too much mental load[9] - while still providing an appropriate level of security.

It is very valuable to have an industry benchmark to compare your number to. Without that, it is difficult to decide whether improvements are essential and even achievable.

In practice, authentication time can be broken down into the time it takes for the app to get an authentication request, the time it takes for the user to understand what the app wants them to do and to successfully provide the user gesture (e.g., touch a fingerprint sensor, look into the camera, or enter a PIN), and lastly, the time it takes for the app to send the authentication response to the server. The breakdown helps to understand where optimization can best be applied.

Making Metrics Actionable

In practice, making metrics actionable requires the most effort. Employees have limited time, so the system needs to make it easy to show the metrics that need improvement and suggest actions to improve them.

Absolute numbers are one thing, but in practice, we often want to focus our energy on the "low-hanging fruit." More specifically, (a) the values that need improvement, and from these values (b) identifying the actions that will bring the "biggest bang for the buck".

Which Values Need Improvement?

Is an average sign-in time of 18 seconds good? Well, it depends. It may be okay for SMS-OTP, but it is likely too slow to use passkeys. But how would you even know that? You could search the internet (e.g., "industry average sign-in time") and might find a result of 29.7 seconds[13]. But is that a good benchmark? Does it apply to customer authentication, or is it a benchmark for workforce authentication? Which authentication method was used? How old is the value, and is it still relevant today?

If you measure the metrics of your company, you can see your trends, and if the trend is in the wrong direction, you might need to act. But you don't know whether you are a leader or a laggard with respect to those metrics, as getting applicable industry benchmarks is either impossible or requires expensive consulting engagements. The company Kellogg recognized the value of industry benchmarks[14] for optimizing general corporate processes long ago and leveraged the work of the American Productivity & Quality Center for that.

It would be meaningful and help drive ROI with the availability of industry benchmarks, such as a benchmark for very specialized electronic processes like sign-in.

Biggest Bang for the Buck

Let's assume you have access to industry benchmarks. You learned that your 18 seconds average sign-in time is way slower than the industry average and your 70% sign-in conversion is also way below the industry average. Additionally, your fraud team keeps complaining about the fraud rate and your customer success manager really wants you to reduce the false decline rate as 42% of consumers say they will be put off from returning to a website following one false decline[15].

Where would you start your journey to improve? Where should you invest time and money to get the biggest return?

The high-level response is easy: Deploy passkeys and reduce reliance on passwords, OTPs, and risk-based authentication methods (which are the main causes of false declines). Adopting these approaches will improve many of these metrics simultaneously[16].

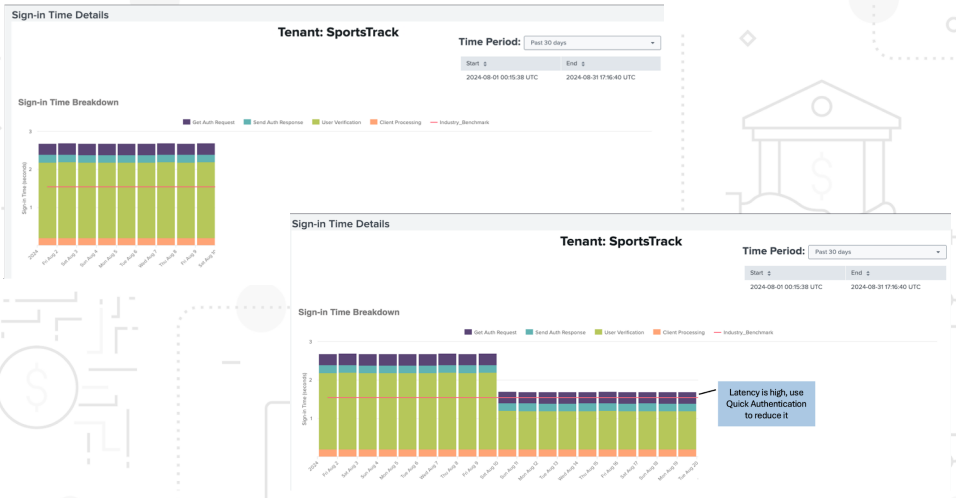
But after that, the devil is in the details. Are you using terminology that users intuitively understand? Are you priming the user correctly to be prepared for the next platform dialog? Have you sufficiently tuned your system? Do you use conditional mediation? Is authentication latency the core issue?

Optimizing the passwordless user experience is not easy - there is a reason why the UX working group is the biggest group in the FIDO Alliance today[17]. Even after implementing passkeys, evaluating how you measure up against industry benchmarks is beneficial. This will provide insights on enhancing your KPIs effectively, considering the resources and budget constraints you face.

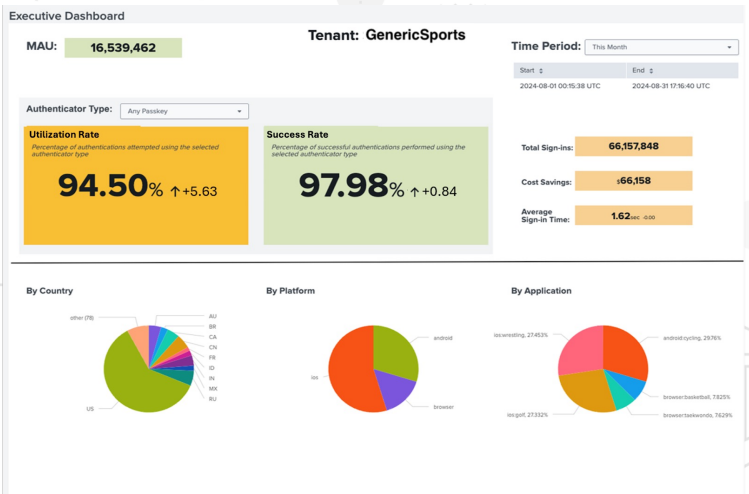
Introducing Nok Nok Smart Analytics

Nok Nok addresses the requirements of collecting and visualizing metrics and trends, comparing them against Industry benchmarks, and making them actionable through its Smart Analytics solution.

Nok Nok addresses the requirements of collecting and visualizing metrics and trends, comparing them against Industry benchmarks, and making them actionable through its Smart Analytics solution.



Nok Nok Smart Analytics measures relevant KPIs and compares your measurements against the “Nok Nok Industry Benchmark” to indicate whether an action should be taken or not.



Nok Nok Smart Analytics provides fine-grained measurements to indicate what should be improved. For example, if it takes too much time for the user to read the dialog and to put the finger on the sensor, you might want to focus on improving the user experience through priming, improved language or other measures.

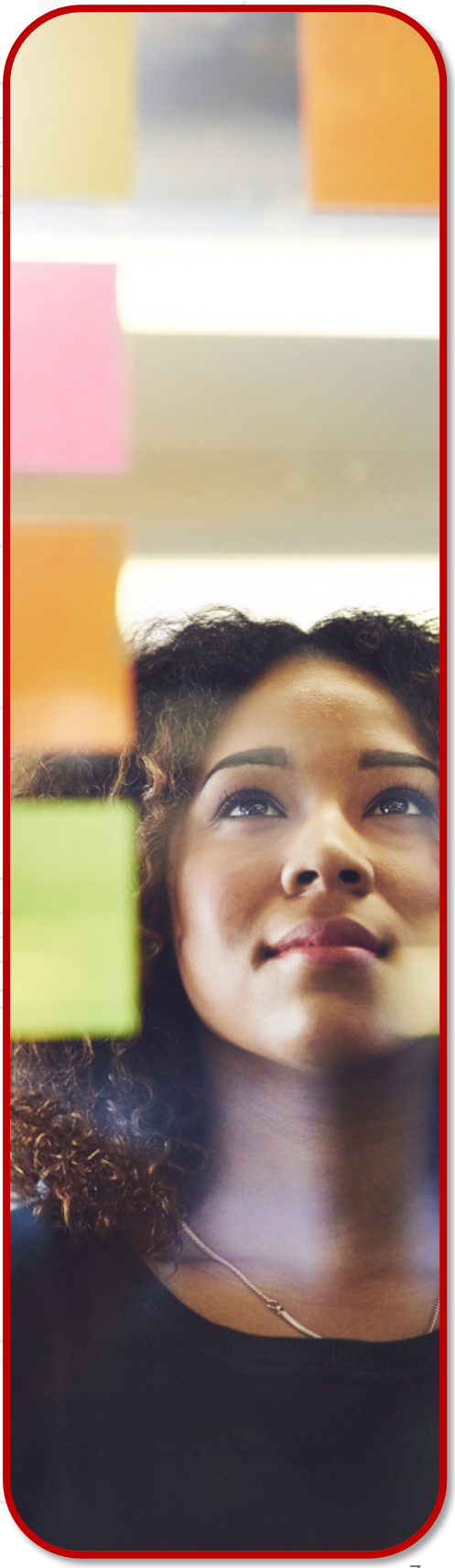
If “authentication latency”, i.e., the time to get the authentication request with the random challenge dominates, you might want to consider using Nok Nok Quick Authentication to significantly reduce it. Nok Nok Smart Analytics actively suggests such improvements.

Additionally, Nok Nok Smart Analytics provides an Executive Dashboard that helps you show your passkey adoption success to stakeholders.

Additionally, Nok Nok Smart Analytics provides an Executive Dashboard that helps you show your passkey adoption success to stakeholders.

Nok Nok Smart Analytics is a powerful solution designed to help organizations optimize their authentication processes by measuring and analyzing key performance indicators (KPIs) and comparing them against industry benchmarks. Smart analytics provides actionable insights to improve user experience, security, and operational efficiency. For example, once deployed, organizations can identify areas for enhancement, such as reducing authentication latency or improving user interaction with sensors, and providing the ability to address specific issues.

Nok Nok Smart Analytics includes an Executive Dashboard that allows organizations to showcase their passkey adoption success to stakeholders, for example. By leveraging AI-driven analytics, the solution not only detects anomalies that indicate fraud risks but also pinpoints deviations in authentication metrics, enabling proactive decision-making. Nok Smart Analytics integrates seamlessly with the S3 Authentication Suite and Authentication Cloud, making it an essential tool for enterprises transitioning to passwordless authentication while maintaining high-security standards.



Conclusion

As cyber threats grow more sophisticated and costly, it's clear that the current approach to cybersecurity is not keeping up. Organizations need to adopt smarter strategies that focus on both robust, phishing-resistant authentication methods like passkeys, and optimize their specific tools and processes. Metrics play a critical role in this effort by providing data to measure performance, identify areas for improvement, and guide decision-making.

As discussed in this brief, key metrics such as passkey utilization rate, registration success rate, authentication success rate, authentication time, and fraud rates offer valuable insights into the effectiveness of authentication systems. However, collecting these metrics is only part of the solution. Making them actionable — by identifying areas that need improvement and focusing on changes that deliver the greatest impact — is essential for driving meaningful results.

By leveraging tools like Nok Nok Smart Analytics, organizations can benchmark their performance against industry standards, pinpoint opportunities for optimization, and make informed decisions about their security strategies. Ultimately, adopting a data-driven approach to cybersecurity not only reduces risks but also enhances user experience and builds trust in an increasingly complex digital world.

1. https://blogs.worldbank.org/en/education/you-can-t-manage-what-you-don-t-measure
2. https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment/
3. https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024
4. https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/
5. https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/
6. https://www.slideshare.net/slideshow/fido-alliance-osaka-seminar-passkeys-and-the-road-ahead-pdf/269440445#1
7. https://youtu.be/8HLBtDtFILI?t=1309
8. https://www.uxdesigninstitute.com/blog/ux-kpis-and-how-to-measure-them/
9. https://www.betterup.com/blog/mental-load
10. https://www.ibm.com/reports/data-breach
11. https://noknok.com/wp-content/uploads/2022/03/Cost-of-Authentication-Failure-Final-1-1.pdf
12. https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study
13. https://www.controlup.com/resources/blog/logon-duration-what-can-be-learned-from-2-million-logons/
14. https://www.wsj.com/articles/how-kellogg-uses-standardized-benchmarks-to-boost-cost-savings-11672953730
15. https://www.checkout.com/guides-and-reports/the-hidden-billion-dollar-opportunity
16. https://noknok.com/wp-content/uploads/2023/03/NokNok-Intuit-CaseStudy_032423_WEB-Version.pdf
17. https://www.passkeycentral.org/design-guidelines/

ABOUT NOK NOK
Nok Nok lets you create safer, faster user experiences with key-based passwordless authentication based on the FIDO standards that enable compliance with global user and data privacy regulations. Nok Nok is the leader in passwordless customer authentication and is trusted by the biggest banks, telcos and fintechs including BBVA, Intuit, Motorola Solutions Inc., NTT DOCOMO, Standard Bank, T-Mobile, and Verizon. For more information, visit www.noknok.com.