onelogin

EBOOK

How to Leverage AI-Powered Multi-Factor Authentication (MFA) For Remote Work

Introduction

With the demand to set up a remote workforce quickly and efficiently, organizations face new challenges around controlling exactly who has access to corporate data outside the safety of the office network.

Authentication plays a central role in cybersecurity and the evolution to Multi-Factor Authentication (MFA) has helped better secure access. But cybercriminals are constantly evolving their tactics – including adding artificial intelligence to their toolkit. As a result, identity and access management (IAM) systems are rapidly implementing very sophisticated AI to further strengthen their security offerings.

MFA provides that critical layer of security and leveraging AI can make the technology more impactful, both in terms of improved security as well as minimal disruptions for end users.

The Importance of MFA for Remote Work

Although traditional MFA is a great first step to securing your users, passwords still remain a weak point. That's because users are notorious for bad password practices such as:

- Reusing passwords
- Using predictable passwords
- Storing password information on sticky notes or in unencrypted spreadsheets

By adding additional factors beyond the password—or, even better, in place of the password—businesses can help thwart password spray and social engineering attacks and stop hackers using stolen credentials from ever entering the account. Additional factors might include answering a security question, using a one-time password, or responding to a push notification on a phone.

However, hackers are clever and even with MFA, people's accounts can be compromised. This is especially true for those users who are working remotely. Devices, like phones or USBs, can be stolen. One-time passwords transmitted via SMS can be intercepted. VPN connections can be exploited to gain access to other vulnerable systems. And biometrics, such as fingerprints and even facial recognition, can be hacked or faked.

But MFA can be improved by adding a critical piece of information:

CONTEXT

Context **is the information about the user's login, like where the user is when attempting to log in or the device being used. Context can provide critical clues that an attack is happening.**

Risk-Based Authentication

To add context, the identity and access management industry has responded with risk-based authentication. Standard MFA captures information about what the user knows, like a password, what the user has, like his or her phone, and even who the user is via biometrics such as fingerprints. Risk-based authentication allows for additional factors that help determine if the user really is who they say they are. This is done by comparing their past login behavior to the current authentication attempt, providing the context that is missing in standard MFA.

For example, if a user usually logs in with a laptop using their home WiFi network, but suddenly tries to log in from a phone in a different country a few hours later, that action may be a sign of a stolen device or worse–a compromised account. You can then ask for an additional authenticating factor, like a one time password or face scan from a token device. Assessing authentication data like this in real-time requires intensive and sophisticated processing.

That's where artificial intelligence comes in.

Enter Artificial Intelligence

As we've seen with COVID-19, setting up a fully remote workforce can lead to a milieu of daunting security challenges. Without the safety of the office network, your users are now accessing sensitive corporate data from locations that you can't control and from WiFi connections that you didn't secure.

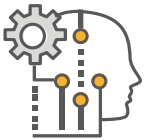
To implement risk-based authentication, companies, like OneLogin, use AI-backed technologies. The AI assesses and weighs individual factors about the login attempt and creates a risk score for the scenario. And then based on the risk score, the technology determines what factors it will ask the user to provide in order to gain access–or, depending on the risk score, it might deny the user access altogether.

How does AI help provide better, more secure authentication?

Risk engines, like OneLogin's Vigilance AI™, monitor a number of factors in a user's login attempts over time and build a profile for each user to understand patterns. When a user varies from that profile on a given authentication attempt, the AI system assesses the variable factors and determines a risk score for the current login attempt.

Some of the factors typically accounted for include:

- Network reputation
- User's geographic location
- The device fingerprint
  (such as the manufacturer, model, or browser)
- Time of login



The final output of the analysis is a risk score that can dictate actions. For example, based on the risk score, OneLogin's SmartFactor Authentication™ adjusts authentication requirements. If the risk score is high, OneLogin might ask for another authentication factor like a fingerprint scan. Or, depending on your settings, the platform might deny the login entirely.

While the key benefit of AI-powered risk-based authentication is security, it can also streamline the authentication process, which is important when all of your employees are consistently accessing your networks from remote locations. With standard MFA, users are prompted for additional factors at every login attempt. Enter your username and password, then answer a security question. Or enter your username and password, and then respond to a push notification on your phone. With AI-powered authentication, low risk users might not be asked for any additional factors, making login faster and less painful.

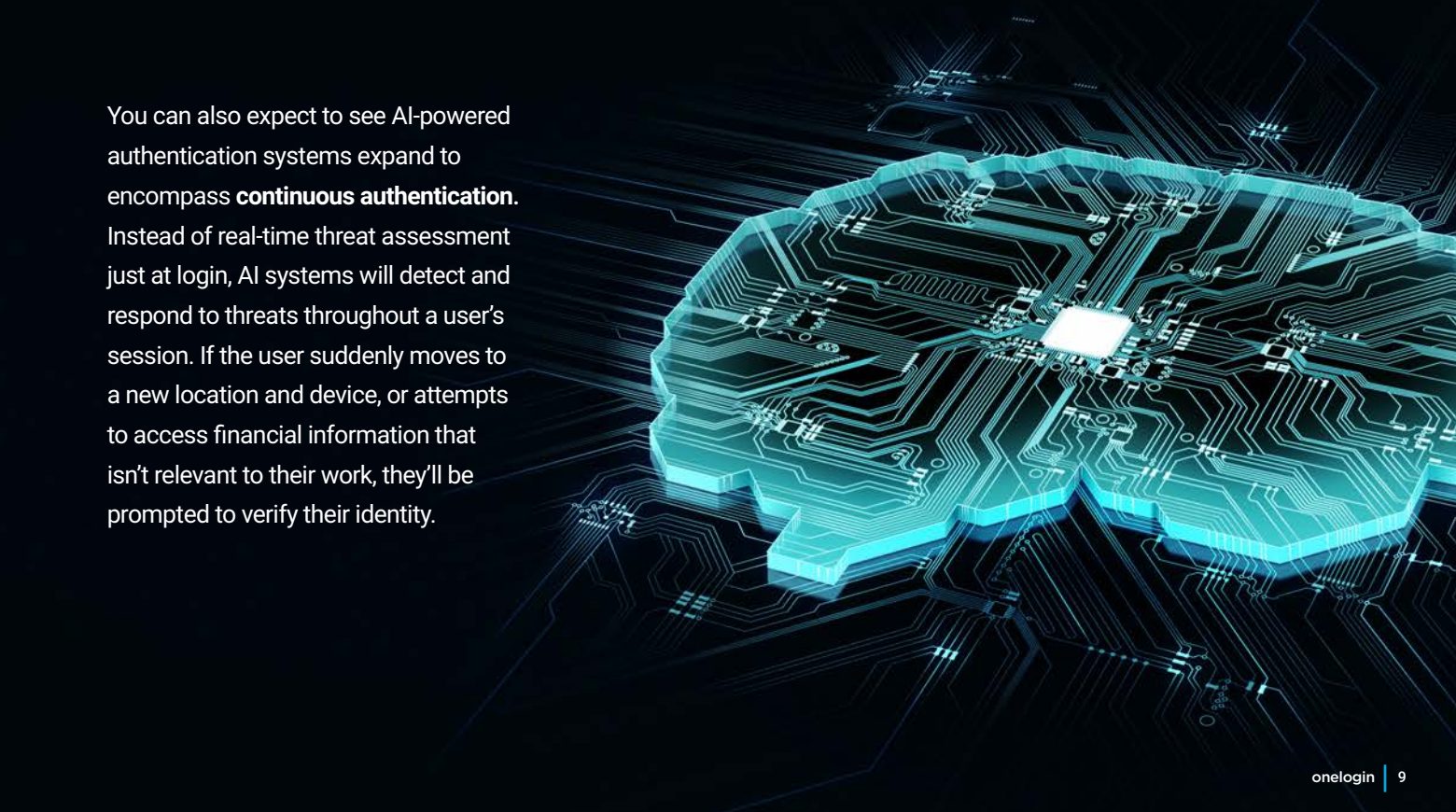
The Future of AI and AUTHENTICATION

As the future of work continues to evolve and change the way people interact with technology, AI and machine learning will continue to bring new ways to accelerate efficiencies and offer rich insights that improve the speed and agility of how work gets done.

Risk-based authentication will continue to improve and get smarter so companies can better protect themselves without slowing their users down. Eventually, authentication that leverages AI will likely move from supervised learning, where the dataset includes the outcomes, to unsupervised learning where the AI finds new patterns to use for making predictions that humans may not have discovered. Cross referencing multiple machine learning algorithms, using pattern recognition, and leveraging time-series-based predictive algorithms will improve the accuracy and scope of AI-based authentication offerings.

At the same time, developers will look for ways to give IT departments more control over the AI system, such as the ability to understand exactly what data went into a given decision, adjust the number of factors being considered, and tailor the system to their organization's unique environment. One area that companies, like OneLogin, are already investigating is the ability to consume third-party data. OneLogin's SmartFactor Authentication includes a compromised credential check that uses third-party data on stolen or exposed credentials. Additionally, various cross-industry initiatives are underway to enable better data-sharing so that the information one organization has on a potential threat can be made available to other organizations in real-time.

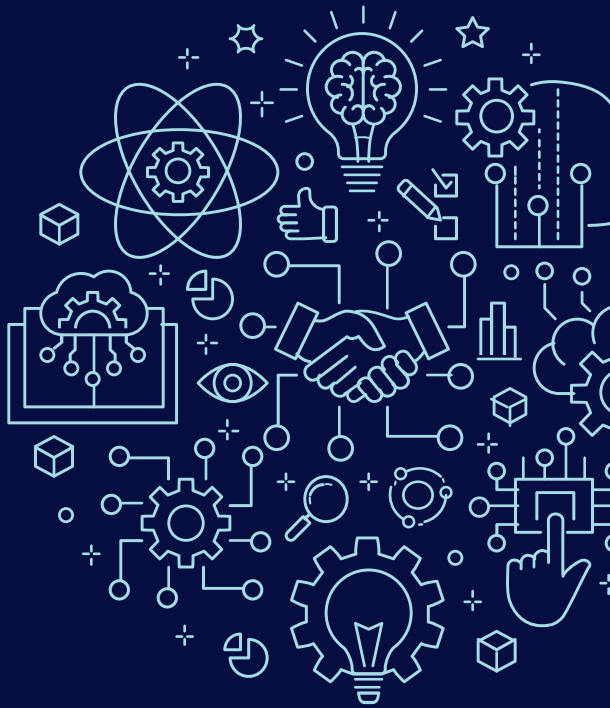
You can also expect to see AI-powered authentication systems expand to encompass **continuous authentication.** Instead of real-time threat assessment just at login, AI systems will detect and respond to threats throughout a user's session. If the user suddenly moves to a new location and device, or attempts to access financial information that isn't relevant to their work, they'll be prompted to verify their identity.



And even further out, access management will likely move from the application level to the data level. Experts are already talking about attaching metadata to individual pieces of data to indicate who should have what type of access to that discrete piece of information. For example, the field in a database containing employee salaries would have metadata indicating that only users within the company who hold certain roles can view that information. Whenever that salary information is exported or shared, the restrictions on access would also be shared. AI-powered authentication would then enforce these data-level access restrictions wherever the data is used.

Conclusion

As identity and access management requirements evolve to meet an increasingly dynamic workforce, how AI is leveraged in IAM will also evolve. Artificial Intelligence will become more necessary to manage the complexity of analysis at the scale and speed of business. Although the first step to ensuring that your remote workforce remains secure is implementing traditional MFA, AI-powered MFA provides more sophisticated protection for the long term.



About OneLogin

OneLogin is the identity platform for secure, scalable, and smart experiences that connect people to technology. With the OneLogin Trusted Experience Platform, customers can connect all of their applications, identify potential threats, and act quickly. Headquartered in San Francisco, CA, OneLogin secures over 2,500 customers worldwide, including Airbus, Stitch Fix, and AAA. To learn more visit **www.onelogin.com**.