SPOTLIGHT

Sponsored by: Thales

Today's identity security landscape is the culmination of decades of technology development aimed at meeting the needs of diverse user groups. Effective multifactor authentication systems must support a wide range of devices, protocols, and platforms.

Why It's Time to Modernize Multifactor Authentication Systems

August 2022

Written by: Jay Bretzmann, Research Vice President, Security Products

AT A GLANCE

WHAT'S IMPORTANT

Modern authentication is already a top investment area for identity security, with multicloud implementations grabbing the lion's share of available funding.

KEY TAKEAWAYS

Piecemeal identity management development over the past 30 years makes it impossible to pick one multifactor authentication (MFA) technology for all user personas and applications. Adoption is estimated to be no greater than 50% within large organizations despite official and unofficial edicts.

Introduction

C-suite executives and outside observers often find it hard to understand why identity security systems are so complicated. There used to be only two categories of users: administrators and regular employees. The application of computer power was limited to automating time-consuming and repetitive tasks, whether that meant calculating ballistics trajectories or processing back-office accounting transactions. Furthermore, only administrators and regular employees logged in to systems and not networks, which operated within protected environments. While this approach was hardly beneficial from a personal productivity standpoint, identity security was pretty easy back then and problems were limited to people who had forgotten that one password someone likely gave them.

Today, there aren't many people — employees, partners, customers, and citizens — who don't use some type of computing technology for most of what they do. Currently, they use a variety of devices and log-ins to both private and public networks that interact with dozens of applications serving up classified, confidential, private, and public data. And for many of these new users and use cases, alternative and proprietary forms of identity security — many of which still exist today — were invented to protect these environments.

Consider the example of a large-scale, vertically integrated manufacturing organization that produces goods leveraging some intellectual property it possesses. The organization employs at least a dozen categories of users assisted in their jobs by both information technology (IT) and operational technology (OT) systems. The needs of the frontline workers are very different from those of the back-office people, the engineers, the human resources team, the executive managers, and so forth, all of whom were probably given access to systems and solutions over dozens of years. This type of environment includes almost as many identity security repositories with differing access and authentication protocols as it has user groups.

But members of the C-suite and the general public watch the news and read the headlines, all of which call for tightening user access and protecting against outside attackers. Some have even been hacked themselves (phished) or had their accounts taken over and data encrypted (ransomware), and they are looking to security teams to "just fix it." Funding issues aside, security teams struggle to understand the depth of their own environments and further devise a plan that will work at least for some user groups.

Modern Authentication

Identity security vendors have been working on such a fix for at least 20 years and have collaborated and developed more standardized technology that many can integrate with a little bit (sometimes a lot) of coding. The newer IT technologies include LDAP/AD, SAML, OIDC, and FIDO2, but CISC/RACF, Kerberos, NTLM, RADIUS, and others still exist in most large enterprise and government environments. When OT protocols (SCADA, RS-232 and RS-485, Modbus, DNP3, HART, TASE 2.0 and ICCP, CIP, PROFIBUS and PROFINET, FOUNDATION Fieldbus, BACnet, etc.) are added to the mix, the extent of the problem becomes clearer. Of course, not all these systems are connected to a network that is vulnerable to attack, yet increasingly systems are connected because bringing an OT system online is cheaper than sending a truck out to a field location.

Modern access control and authentication requires injecting more signals or intelligence into both the requestor (user) and the relying party (service). Many vendors refer to this capability as "contextual" or "adaptive" authentication because it leverages telemetry such as user location, time of day, device health, and even prior behavioral practices. Contextual information can also feed into a continuous authentication capability that reissues a challenge when conditions change over a defined period of time. Modern authentication also requires multiple authentication devices ranging from smartphones to platform authenticators and hardware security keys to software tokens.

The use of asymmetric encryption (aka public key infrastructure [PKI]) is another powerful means for modernization helping avoid so-called man-in-the-middle (MITM) attacks where users can't positively identify the source of an identity challenge request. Said another way, smart people got together and agreed on some technical stuff. Newer protocols — FIDO2 — implement these ideals while older approaches generally need some sort of intervening service or gateway to broker such communications. The more secure PKI approaches generate keys using Trusted Platform Modules (TPMs) on local devices where the private key never leaves the local system; however, this approach is not always possible because some supported devices may not have such processing capabilities. In that case, a centralized key management system is required, and the private keys are distributed to the endpoints where they are stored in specialized enclaves.

Most enterprise organizations — especially government agencies — can't simply decommission all their legacy applications and mothball on-premises identity stores. They still need authentication methods that use older authentication protocols (NTLM, Kerberos) that may be protected via smartcards (PIV/CAC) or, better yet, implemented via a reverse proxy approach where authentication is performed before application access is allowed. Very few organizations are either in a position (skills) or brave enough (guts) to rewrite older application access methods.

Cloud and Legacy Deployments

Early "lift and shift" efforts migrating applications to the cloud uncovered a new set of security challenges for organizations trying to benefit from infrastructure (IaaS) savings. VPNs and jump servers were access methods that didn't properly scale and were a single point of entry to the network exposing all available services. Access management tools developed by cloud service providers (SPs) worked only within their cloud while the world was overwhelmingly building hybrid multicloud environments (81% of organizations per *The 2020 State of Identity Security in the Cloud*, a study published by the Cloud Security Alliance).

A centralized resource for controlling access and authentication that could work with all cloud SPs and SaaS applications (Workday, Salesforce, etc.) fast became a hard requirement, but an approach that could also incorporate legacy on-premises applications was even better. When it comes to identity management, visibility is a key evaluation consideration for most organizations to reduce both unforeseen exposures and traditional overprovisioning practices, which organizations often pursue to ensure that people can do their work. The Cloud Security Alliance study identified multifactor authentication (MFA) technology as the top identity investment priority, with an expected 85% increase in spending over the coming 12 months.

Services Are Often Required

IDC can safely predict that despite identity technology standardizations and ever-increasing application integrations, any large organization working to modernize its identity security solutions will face the need for additional deployment and tuning services as security teams uncover undocumented APIs and potential data exposures that impact employee and user privacy. Furthermore, one of the biggest challenges for tightening identity security measures is user resistance because organizations know more friction is coming in two forms: access denials and quirky or annoying user interfaces. Given the complexity of their environments, such resistance is — and always has been — inevitable.

Definitions

Multifactor Authentication

MFA is an identity security technology that requires multiple methods of authentication from independent categories of credentials to verify a user's identity for a log-in or other transaction. MFA combines two or more independent credentials: what the user knows, such as a password; what the user has, such as a security hardware/software token or registered device; and who the user is, such as geolocation, time of day, knowledge of previous interactions, or biometric verification methods.

Man-in-the-Middle Attack

An MITM attack is based on the ability of an attacker to fool victims into thinking that they are interacting with a legitimate website or service ("relying party" in WebAuthn parlance) when in fact they are not. As the user (requestor) logs in to the service, they typically disclose a username/password combination. The attacker then uses those credentials to establish separate communications with the real service provider. If a second identity factor is required, the attacker then notifies the oblivious requestor, and the real service sends a direct challenge to a pre-registered authenticator completing the identity circle. The attacker is now in control since the service never included user identifying credentials and the browser never included domain name information when communicating with the authenticator.

Phishing

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. These attacks are usually performed through email and often include personal details collected from social media and other professional websites to trick a user into action. The goal is to easily breach the network and find and steal sensitive data (credit card numbers and log-in information) or install malware on the victim's machine such as a remote access trojan (RAT). Phishing tactics always top the list as the most common type of cyberattack, according to Verizon's long-running *Data Breach Investigations Report*.

Public Key Infrastructure

A public key infrastructure is a set of roles, policies, and procedures needed to create, manage, store, and revoke digital certificates for an asymmetric encryption technology. PKI use cases include network Transport Layer Security (TLS) data encryption, confidential email systems, and secure identity management systems. PKI uses public and private key pairs as opposed to a symmetric approach such as Kerberos.

Benefits

Identity is a foundational element for all IT security, but only if it's done right, which means positively identifying who or what is requesting access to a network's services without causing a widespread revolt. A modern approach to authentication means retiring free or near-free methods that rely upon single factors (passwords) or easily phishable second factors (SMS) in favor of technologies that leverage signals, intelligence, and encryption to better document a service requestor, whether person or machine.

Given that identity is foundational, it should be easy to choose a new approach that incorporates more stringent requirements. Yet a universal solution doesn't exist. Logging in to a financial or healthcare system requires a bot-resistant approach that is different from that for email, chat, and file sharing services. If the solution further requires the development of a whole new protocol (open, documented, and standardized these days), set your commercial viability expectations to be a decade hence.

Next, you need to understand and plan for physical access restrictions due to where a user is and what that person is using to initiate contact. Gowned, masked, and gloved individuals can't easily perform authentication checks designed for an office environment. In areas where cellphone use is prohibited, getting an OTP code is likely not a possibility, even if you can request one via Wi-Fi.

Whenever possible, modern authentication should employ certificates in much the same way all secure (https) web applications do by using TLS or administrators to accomplish remote log-ins with SSH keys. Certificates can be purchased from a certificate authority and vaulted or, better yet, locally generated by an endpoint agent or a biometric device and stored in a secure enclave. For peak security, keys must be managed, rotated, and deleted in a timely manner once they are no longer required.

Yet not every use case scenario will be served by these strongest forms of MFA. Studies have shown that even deploying push technology (codes, checkmarks, or QR codes) to email addresses or smart devices will help eliminate the vast majority of today's successful phishing attacks. Most larger organizations will be required to do multiple forms of MFA to cover all their use cases.

Trends

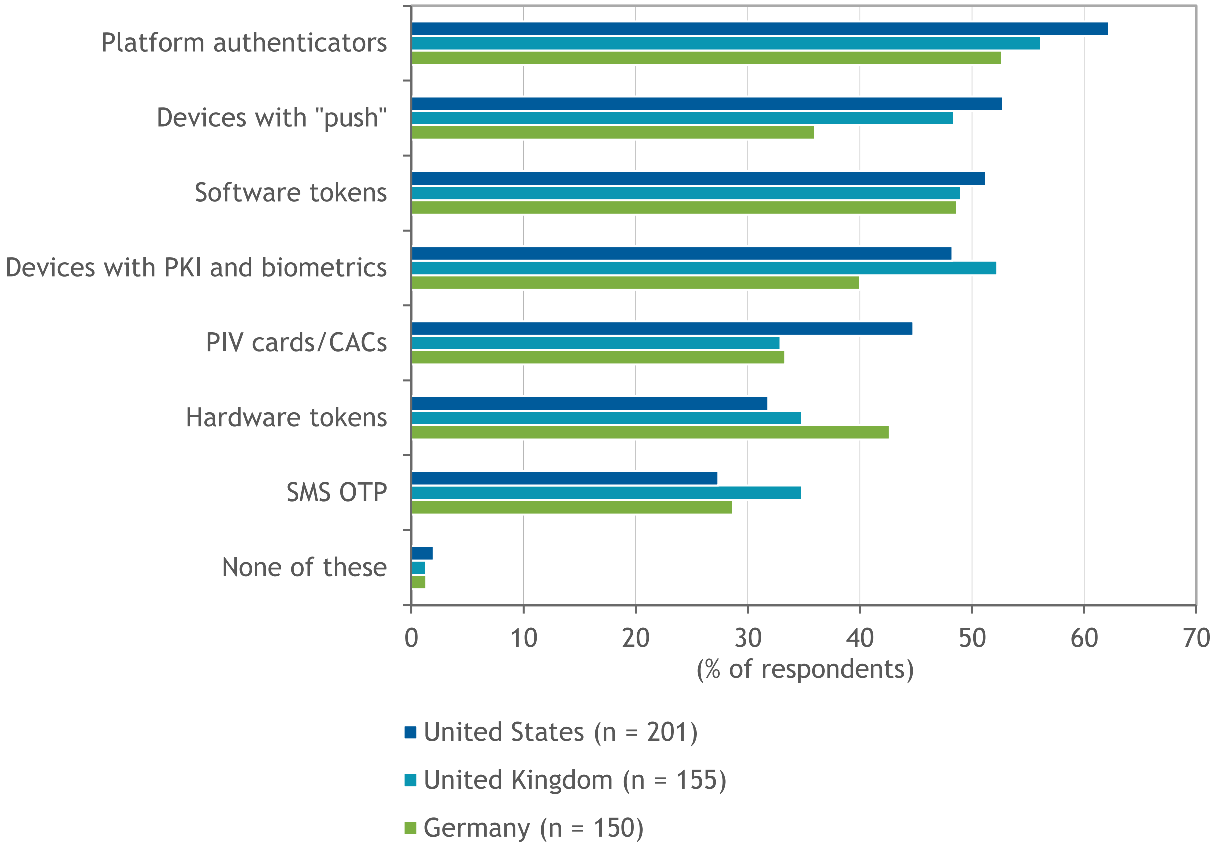
As modern authentication technology is increasingly recognized as vital to a zero trust networking environment, there are new calls from the U.S. federal government and European Commission to improve adoption rates. IDC believes no more than 50% of organizations have currently deployed even the simplest forms of MFA mainly due to funding limitations. Executive orders and OMB memos aside, departments and entities will have to make their cases for interim funding from the Technology Modernization Fund (TMF), which has historically operated under a full repayment model and will continue to do so for projects that yield financial savings realized by the proposing agency. The TMF board expects this to apply to "single-agency investments with direct cost savings, such as replacing a legacy system with one that can be operated and maintained more efficiently."

Biometric (finger, face, voice) reading devices and behavioral monitoring solutions already exist but require smart devices; however, not everyone owns a smart device, and such devices are neither allowed in all workplaces, healthcare settings, and governmental facilities nor accessible in remote geographic locations. FIDO2 changed the game for secure access to many web applications, but initial device registrations still required a password in most cases. Today the enduring issue is one of device recovery, and the FIDO Alliance is working with Microsoft, Apple, and Google to fix this problem using a "passkey" approach where the credential is stored within a cloud keychain rather than a single, registered device. Termed "Multi-device FIDO," most implementations are still rated as nonproduction previews.

Platform authenticators (Windows Hello and Google Authenticator) are helping employees using laptops and workstations go passwordless while social media log-ins (Facebook, Twitter, LinkedIn) are doing the same for consumers. See Figure 1 for multifactor authentication usage trends.

FIGURE 1: ***Multifactor Authenticator Usage by Geography***

Q *What primary forms of advanced authenticators (multifactor/two-factor authentication) are in use at your organization?*



Base = all respondents

Note: Multiple responses were allowed.

Source: IDC's Security Identity Survey, September 2021

Considering Thales

Thales' Digital Identity and Security Division offers a range of products spanning the digital and physical worlds using three business units (Cloud Protection and Licensing, Banking Payment Services, and Identity and Biometric Services) to address workforce, B2C, and B2G opportunities.

In terms of offering a full identity and access management (IAM) stack, Thales is continuing to evaluate feature/function adjacencies the company can add to the core advanced authentication solution using a cloud delivery rather than a separate packaging approach. Identity proofing, self-service user capabilities, improved directory integrations, and single sign-on are some relevant examples of use case–oriented investments. The company is also actively contributing to the CAEP/SSE OpenID standards effort to enhance its risk management capabilities and improve its zero trust competitiveness.

SafeNet Trusted Access is the ready-made cloud-based service from the Gemalto acquisition, offering similar features and complemented by scenario- and risk-based access policies. This service now contributes more than half of all identity revenue. The solution supports every form of authentication technology available in the market today and can leverage technology across multiple business units to deliver unique capabilities to large enterprises. Thales has access to a €1 billion research and development fund for the broader organization and has offered passwordless identity options for at least a decade. It holds a dominant market share position in the European Union market and is an independent supplier of security software.

In addition to Thales' identity solutions (which make up the vast majority of the company's security software revenue), another major pillar of the vendor's portfolio is information and data security solutions, with a range of both hardware appliances and software. These two pillars provide complementary capabilities from a security and risk management perspective. For example, Thales CipherTrust Data Discovery and Classification provides data discovery, classification, and risk analysis across heterogeneous data stores (both cloud and on premises). The solution can identify, for example, PCI DSS– or GDPR-regulated data and encrypt it, with all keys managed through a central platform. Combined with Thales' identity management, authentication, and access controls, these solutions can go a long way to helping customers pass compliance audits. Consequently, the company has built up a major customer base among banking and payments-related firms, government entities (particularly in relation to digitalization and regulations such as eIDAS), and critical infrastructure companies.

In July 2022, Thales took steps to broaden its identity security portfolio with a B2C/B2B solution by acquiring the Dutch company OneWelcome for a total consideration of €100 million. OneWelcome provides cloud-based customer identity and access management (CIAM) for highly regulated industries, empowering them to securely connect customers as well as business partners to their online services.

Prior to the OneWelcome acquisition, Thales announced a definitive agreement with Sonae Investment Management to acquire two other leading European cybersecurity companies, S21sec and Excellium, owned by the holding company Maxive Cybersecurity. These organizations complement Thales' cybersecurity portfolio, strengthening the vendor's incident detection and response services (Security Operations Center — SOC) as well as consulting, audit, and integration services. The two companies will also bring extensive expertise and a diversified customer base of industrial companies and critical infrastructure providers.

Challenges

Thales supports several authentication technologies, which speaks to its dedication to supporting enterprise organizations, yet it lacks the behavior biometrics that many other vendors have developed for passwordless and continuous authentication use cases. From a competitive positioning standpoint, Microsoft and Okta are bigger voices in the market, and though both are expanding their platform solutions, many organizations are using best-of-breed MFA vendors to address their diverse authentication requirements. Thales' deep focus on identity authentication and data security plays strongly in several vertical markets, but IDC believes complementary identity governance is growing in importance for managing access over longer-term identity life cycles.

Conclusion

Interest in and adoption of modern authentication solutions continue to grow as older forms of identity access management are increasingly ill-suited for a COVID-19-induced distributed workforce. Most organizations inherently know this yet face multiple challenges finding solutions that can fit increased user diversity and growing IT complexity. Identity projects are just difficult — even for midmarket companies — as on-premises, IaaS, and SaaS applications all tend to require different access methods.

IDC believes organizations will be modernizing their identity infrastructures for the next 5–10 years and expects MFA adoption to become as prevalent in the next three years as single sign-on is today. These solutions are closely linked and some of the easier IAM components to be hosted as a service.

Interest in and adoption of modern authentication solutions continue to grow as older forms of identity access management are increasingly ill-suited for a COVID-19-induced distributed workforce.

About the Analyst

***Jay Bretzmann,** Research Vice President, Security Products*

Jay Bretzmann is Research Vice President for IDC's Security Products service responsible for Identity and Digital Trust and Cloud Security. Jay focuses on identity management, privileged access management, identity governance, B2C identity management, and a multitude of other identity and cloud security topics.

MESSAGE FROM THE SPONSOR

About Thales

Today's enterprises depend on the cloud, data and software in order to make decisive decisions. That's why the most respected brands and largest organizations in the world rely on Thales to help them protect and secure access to their most sensitive information and software wherever it is created, shared or stored – from the cloud and data centers to devices and across networks. Our IM solutions enable organizations to move to the cloud securely, modernize their IT environments and achieve compliance with confidence. To learn more about the SafeNet Trusted Access visit https://cpl.thalesgroup.com/access-management/safenet-trusted-access.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.