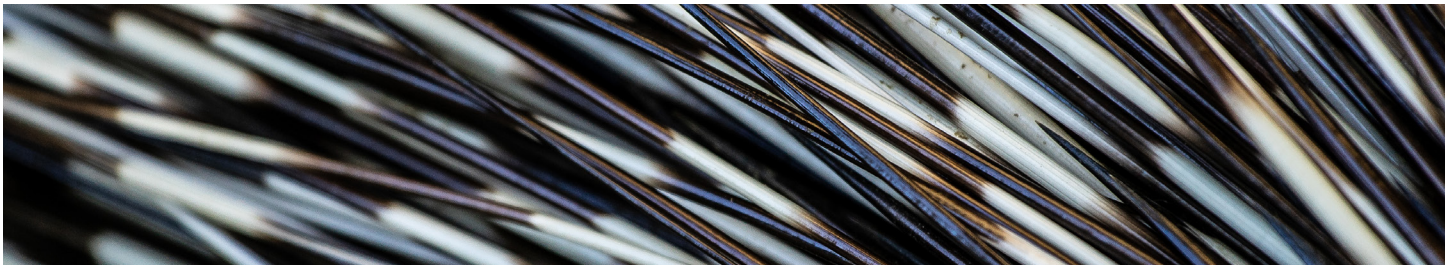

Proving identity and protecting credentials in a work-from-anywhere world

Many businesses continue to rely on outdated verification and access management models that leave their networks exposed — a situation only exacerbated by remote work.

Key takeaways

- Hybrid work environments have introduced many new vulnerable access points to the corporate network, requiring an increase in credential security.
- Stand-alone modes of verification, such as "trust, but verify" need to be augmented by architectural additions to protect a distributed workforce.
- Best practices for credential security today include single sign-on (SSO), multi-factor authentication (MFA) and least-privileged access, as well as updated security software and employee education.
- The future model for corporate credential security may render passwords obsolete, instead moving to behavioral biometrics or just-in-time access.

It's no secret that the pandemic-driven shift to remote work has dramatically increased cyber security risk for most businesses. The sheer number of new entry points introduced by remote personnel — including personal devices, public Wi-Fi networks, home networks and Internet of Things (IoT) devices — vastly increases an organization's threat surface. In addition, many work-from-anywhere (WFA) devices and networks are under-secured, with minimal or no identity verification required. Add to that a remote workforce that may not be up to date on the latest WFA best practices, and you have the perfect storm for a security incident.

Cyber criminals are, unfortunately, more than aware that remote work has weakened businesses' security postures. A dramatic rise in cyber crime has paralleled the adoption of remote and hybrid work, especially crime targeting credentials. The associated costs of security incidents have also skyrocketed, with remote work leading to incidents that are, on average, over $1 million more expensive than those for which remote work was not a factor.[1] With compromised credentials cited as the most common cause of security events, it's clear that organizations need to re-envision how they protect credentials and prove identity when providing access to remote employees.

[1] IBM Security and Ponemon Institute, "Cost of a Data Breach Report 2021," July 2021.

"Trust, but verify" comes up short

Traditional on-premises corporate security allowed internal traffic to assume trust. Swipe a badge, gain entry. Match the face on that badge, stay in the building. This trusted access extended to all systems and networks, empowering organizations to follow the "trust, but verify" model, in which users were given full access to the corporate network once their log-in credentials were validated. As cyber crime tactics advanced, however, this approach was akin to providing bad actors with the keys to the castle: If criminals had just one employee's credentials, they could gain access to the entire network, including sensitive financial or proprietary data.

In fact, a proliferation of criminal methods for targeting credentials has arisen, ranging from technical tactics like keylogger malware and credential-harvesting tools to social engineering techniques, such as spear phishing and business email compromise. With remote work transitioning from a temporary stopgap to a business-as-usual mainstay, businesses need a security model that can better adapt to today's threat landscape.

Best practices for credential security today

Improved password hygiene

In 2020, a whopping 82% of people admitted to reusing their passwords across multiple accounts[2] and often across work and personal accounts.[3] That same year, about 20% of breaches were caused by compromised credentials.[4] So it's no surprise that login credentials alone provide only a façade of security.

With criminals increasingly targeting stolen account credentials and using them to gain access to other accounts and services — also known as "credential stuffing" — preventing password reuse and requiring stronger, more frequently updated passwords is a first step to improving credential security.

- **Prevent password reuse** by using policies that store old passwords and restrict repetition.
- **Set maximum password age limits** to ensure passwords are changed — and minimum age limits so they can't be quickly changed back.
- **Require that passwords meet complexity requirements** — i.e., contain at least one uppercase and lowercase letter, one number and one special character.
- **Set minimum password lengths** and encourage employees to create long passphrases unrelated to personal information (no birthdays, street numbers, names, etc.).

Multifactor authentication (MFA)

Stolen or compromised credentials are one of the top causes of data breaches, with 61% of incidents involving user logins.[5] Given that criminals have access to so many credentials, requiring a secondary layer of identification through multifactor authentication is a good idea to help thwart unauthorized access. MFA should require at least two methods of identification, which could include:

- **Something the real user knows:** Information only the user would have knowledge of, such as a password, personal identification number (PIN), a one-time password (OTP) or answers to personal security questions.
- **Something the user has:** A physical object only the user is in possession of, such as a security token, USB device, smart card or smart phone.
- **Something the user is:** Unique physical characteristics of the user, such as fingerprints, facial recognition, voice recognition, retina scanning or other biometrics.

[2] IBM, "2021 Data Breach Survey," 2021.
[3] SpyCloud, "2021 Annual Credential Exposure Report," March 2021.
[4] IBM, "2021 Data Breach Survey," 2021.
[5] Verizon, "2021 Data Breach Investigations Report," May 2021.

Single sign-on (SSO)

Not only is credential theft a key contributor to security breaches, but so is password fatigue. When users are prompted to change passwords frequently, all too often they make simple changes, such as switching out one character or adding a character to an existing password. Using SSO authentication — i.e., allowing one set of login credentials to access multiple systems — can mitigate risk by reducing both password fatigue and credential theft. When implemented securely (e.g., in combination with MFA), SSO benefits include:

- **Reducing password fatigue** by eliminating re-entry of passwords.
- **Minimizing risk** when accessing participating third-party sites because passwords are no longer stored externally.
- **Reducing the risk** of criminal access to multiple passwords.
- **Decreasing the likelihood** that users will store passwords insecurely (e.g., by writing them down).

Least-privileged access

One of the most dangerous aspects of credential compromise is that once cybercriminals gain access to your network with even a low-level user login, they can exploit that access to gain elevated privileges across the entire network. Adhering to a principle of least-privileged access can help limit damage from a hacker or malicious insider with unauthorized access.

- **Restricting users' access rights** to only the data and systems they need to perform specific tasks is one of the best ways to limit damage from incidents.
- **Least-privileged access** can be used with segregation of duties policies to limit users' access to specific functions.

Zero trust

As remote work has physically removed employees from the office, as well as dramatically increased the number of entry points for cyber criminals to exploit, it's become harder to verify both the identity and security status of all the users and devices connecting to your networks. Traditional perimeter-based security is no longer enough and even least-privileged access may allow malicious actors to gain a foothold from which to escalate their access privileges. An even more secure approach is the zero trust security model.

- **Zero trust access follows a "never trust, always verify"** concept, in which every user and device must be continuously validated before receiving access and access is only given on a per-request basis.
- **Rather than focusing on perimeter defense** and authorizing access across a collection of resources on a network, zero trust focuses on granting access to specific resources, and only on an as-needed basis.
- **Users and devices are never provided trust by default,** even if they have previously been connected to company resources.

Employee education

Additionally, education of remote/hybrid workers in two key areas is critical:

- **Processes:** Establish clear processes for all interactions with company resources to reduce risk of compromise through social engineering. For example, ensure employees have clear guidance on how, when and why an IT representative would contact them — and what information should and should not be provided — to avoid phishing (email), vishing (voice), and smishing (text message) scams.
- **WFH policies:** Create and distribute policies and recommendations for securing home networks and personal computing devices. By educating remote workers on better cyber hygiene, businesses protect not only their own networks and data, but the digital lives within employee households.

By incorporating process and policy changes with education, companies can help employees see the value in these additional security steps.

Lastly, organizations need to take a "secure by design" approach, building security into systems and software from conceptualization and design phases, and implementing technologies that provide credential protection through secured user devices (endpoint protection), secured transmission (encrypted data communications) and patched and secured software (data in use).

The future of credential security

Newer guiding principles of credential security support evolving policies and technologies that limit access without limiting functionality. One such principle is just-in-time access, in which users receive access to privileged servers and software on an as-needed (and only-when-needed) basis. This model hasn't yet been widely adopted, but it could be implemented in organizations endorsing the zero trust approach.

Further, many security analysts predict a passwordless future for individuals and organizations. By improving the identity model with uniquely individual identifiers — such as biometrics or behavioral data — organizations could theoretically phase out usernames and passwords for stronger, less duplicable credential security. For example, by using artificial intelligence and machine learning, companies can gather behavioral biometrics on employees — such as typing speed, keystroke dynamics or gait and posture analysis — without user intervention, providing a frictionless and continuous authentication approach.

By adhering to the latest best practices in credential security, identity verification and access management, companies can drastically reduce risk brought on by remote and hybrid infrastructures while building resilience and supporting business continuity. With continuous iteration of process, policy and technologies, organizations can actively adapt to changing threat landscapes and respond in an efficient and effective manner. This, coupled with orchestration systems, machine learning and more efficient data identification and classification, will drive the future of credential security. ■

Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is," with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor.

"Bank of America" and "BofA Securities" are the marketing names used by the Global Banking and Global Markets divisions of Bank of America Corporation. Lending, other commercial banking activities, and trading in certain financial instruments are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., Member FDIC. Trading in securities and financial instruments, and strategic advisory, and other investment banking activities, are performed globally by investment banking affiliates of Bank of America Corporation ("Investment Banking Affiliates"), including, in the United States, BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and Members of SIPC, and, in other jurisdictions, by locally registered entities. BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC and are members of the NFA.

Investment products offered by Investment Banking Affiliates:
Are Not FDIC Insured • May Lose Value • Are Not Bank Guaranteed.

BANK OF AMERICA