CYBERARK®
THE IDENTITY SECURITY COMPANY®

WHITEPAPER

Reimagine Workforce Security for End-to-End Identity Protection

Layered access and privilege controls prevent modern identity-based attacks.

Introduction

The threat landscape is rapidly shifting with the emergence of new identities, environments and attack methods. Cybercriminals are finding new ways to penetrate networks, disrupt business-critical systems and steal confidential data.

Traditional identity and access management (IAM) systems like multi-factor authentication (MFA) and single sign-on (SSO), as a single checkpoint at login, cannot fully defend against today's advanced, identity-based attacks. Adversaries routinely carry out "MFA bombing" attacks, social engineering schemes and other advanced techniques to trick unsuspecting users by circumventing baseline IAM solutions and breach networks.

The 2022 Uber data breach is a classic example of an attacker using a combination of social engineering and MFA fatigue attack to gain access to the network. A year later a popular identity service provider suffered a similar identity-based attack on their case management system using compromised credentials. The incident impacted the provider's entire customer base, exposing confidential information.

IDENTITY: THE EPICENTER OF MODERN CYBERATTACKS

95%

of organizations have experienced two or more identity-related breaches in the last twelve months.[1]

50%

of incident responses in early 2024 were triggered by MFA bypass attacks.[2]

It's worth noting that these are known methods to bypass authentication controls — and attackers are using them to their advantage in places where endpoint and network controls cannot reach. They are exploiting a blind spot – a vulnerability in foundational identity and access management strategy — that only a unified approach to workforce identity security can solve.

[1] CyberArk, "Identity Security Threat Landscape Report," May 2024.
[2] Cisco Talos, "Incident Response Threat Summary," Jan-March 2024.

Reimagining Workforce Identity Security

Going forward, enterprises should take a holistic, identity-centric approach to workforce identity security to defend against modern threats and ensure workers have easy, secure access to all their resources and applications. A comprehensive workforce identity security strategy should account for every attacker pathway, and defend against pre-authentication, at-authentication and post-authentication attacks. Conventional access security controls like MFA and SSO are still critically important, but they are no longer fully sufficient. In today's world, threat actors don't break in, they log in.

The future of access security lies not in simply managing logins, but in providing truly secure access across the entire user journey — from the first point of authentication and beyond. The future of workforce identity security is about delivering layered, intelligent privilege controls™ that extend exactly the right amount of security at the endpoint, within the browser, through to native applications and web sessions. This new paradigm shifts from a rigid, one-dimensional security model to an approach that enables trusted access and transparent, seamless protection.

Securing the Modern Workforce

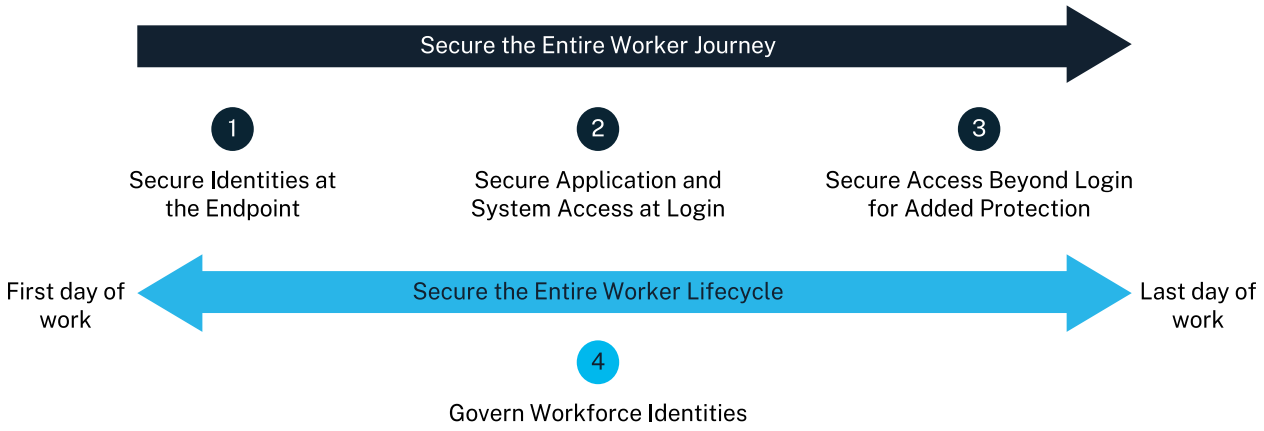
Securing today's dynamic, distributed workforce is no easy task. The modern workforce is made up of a variety of workers (employees, contractors, freelancers, partners, application administrators and vendors) who access an array of applications (cloud-native business apps, conventional on-premises applications, SaaS solutions) from any location (home, the office, or the road) using any device (company-supplied and personal).

Every worker, regardless of their role can be a privileged, high-risk user. Any user can become a potential target based on their rights, their access to sensitive data and their role in critical workflows.

Securing the workforce — protecting every user's identity, managing their privileges, monitoring and controlling their actions, securing their endpoints — is paramount. It's more important than ever to safeguard users' credentials, their browsers and the machines they work on, and closely govern their evolving permissions from their first day on the job to their last.

Four Effective Ways to Strengthen Workforce Identity Security

You can defend against modern identity-based attacks by introducing layered access and privilege controls across the entire user journey, throughout the entire employee lifecycle. An end-to-end approach to workforce identity security safeguards every user interaction, from login and beyond, providing continuous protection against pre-authentication and post-authentication attacks. It manages workers' fluctuating roles and privileges throughout their tenure, improving governance and oversight.



Here are four effective ways to strengthen workforce identity security, defend against modern attacks and mitigate risk.

1. Secure Identities Starting at the Endpoint

The user journey begins at the endpoint. And every endpoint, whether it's a workstation or a server, includes built-in administrative accounts. Adversaries can exploit endpoint vulnerabilities, configuration errors and standing permissions to gain access to privileged accounts, move laterally, and orchestrate attacks. Costly supply chain attacks and ransomware attacks targeting endpoints are commonplace.

Use an endpoint identity security solution to control access and privilege at the endpoint. Endpoint identity security solutions continuously discover and remove local admin rights from workstations and servers and provide just-in-time privilege elevation and fine-grained application controls to enforce the principle of least privilege and limit exposure. They also monitor and detect unauthorized access to passwords, credentials, hashes, cookies and other security tokens thereby improving visibility into suspicious activity symptomatic of an identity-driven attack.

By hardening endpoints and reducing the attack surface, endpoint identity security solutions help defend against zero-day attacks, contain lateral movement and ransomware spread, and mitigate insider and external threats. They also help support Zero Trust security frameworks and provide evidence of compliance and readiness for auditors and cyber insurance underwriters.

2. Secure Application and System Access at Login

Use IAM solutions to authenticate users and control access to critical applications and services at login. Implement SSO to eliminate credential sprawl and reduce your attack surface. SSO gives workers secure access to all applications and systems using a single set of credentials; it reduces exposure while improving user experience.

Implement adaptive MFA to ensure each user is who they say they are. Choose phishing-resistant authentication factors (smart cards, passkeys, push notifications) that best meet your security and usability needs. Use contextual information, such as user risk, location, device and time-of-day to determine which authentication factors to apply to a particular user in a particular situation. Adaptive MFA strengthens security without incumbering users.

Use a password manager to enhance the security of non-federated apps. Password managers reduce vulnerabilities by removing passwords from endpoints and browsers. They also eliminate password fatigue and risky workarounds like workers reusing passwords or tracking them on paper or in clear-text files.

Securely store all credentials in a centralized digital vault for ultimate protection, control and administrative simplicity. Credential theft is a major concern. Over 24.5 billion credentials are circulating on the dark web.[3] Many of them provide access to business-critical applications and systems, and confidential data. Over 80% of organizations have experienced an attack exploiting stolen credentials in the past 12 months.[4]

3. Secure Access Beyond the Login for Added Protection

Securing access at login is fundamentally important, but not totally sufficient. Threat actors can hijack active sessions and exploit privileged identities to exfiltrate data or carry out attacks. Implement step-up authentication and continuous authentication to secure high-risk users beyond the initial login and protect against advanced identity-driven attacks.

Use step-up authentication to re-validate users before they perform high-risk actions like installing software or running applications with elevated privileges. Step-up authentication is crucial for enhancing security, while maintaining usability. It ensures users can perform low-risk actions with minimal friction, but requires additional verification for operations that might be employed in an attack. Step-up authentication helps protect against cookie theft and other types of session abuse and malicious incidents.

Use continuous authentication to re-validate high-risk users after a pre-defined period of time or inactivity. Continuous authentication protects against session hijacking and unauthorized application access and defends against adversary-in-the-middle (AitM) or man-in-the-middle (MitM) attacks. Leading identity security platforms can automatically re-authenticate users if they engage in unusual behavior.

Deploy secure browsers to safeguard access to web apps, SaaS solutions and cloud consoles. You can use a secure browser to block access to unsanctioned URLs, suppress clipboard functionality, prevent file transfers and restrict browser extensions. Secure browsers help combat malware and data exfiltration and mitigate cookie theft and browser-in-the-middle attacks.

---

[3]Dark Reading, "24 Billion Credentials Circulate on the Dark Web in 2022," June 2022.
[4]CyberArk, "Identity Security Threat Landscape Report 2024," May 2024.

4. Govern Workforce Identities Across the Lifecycle

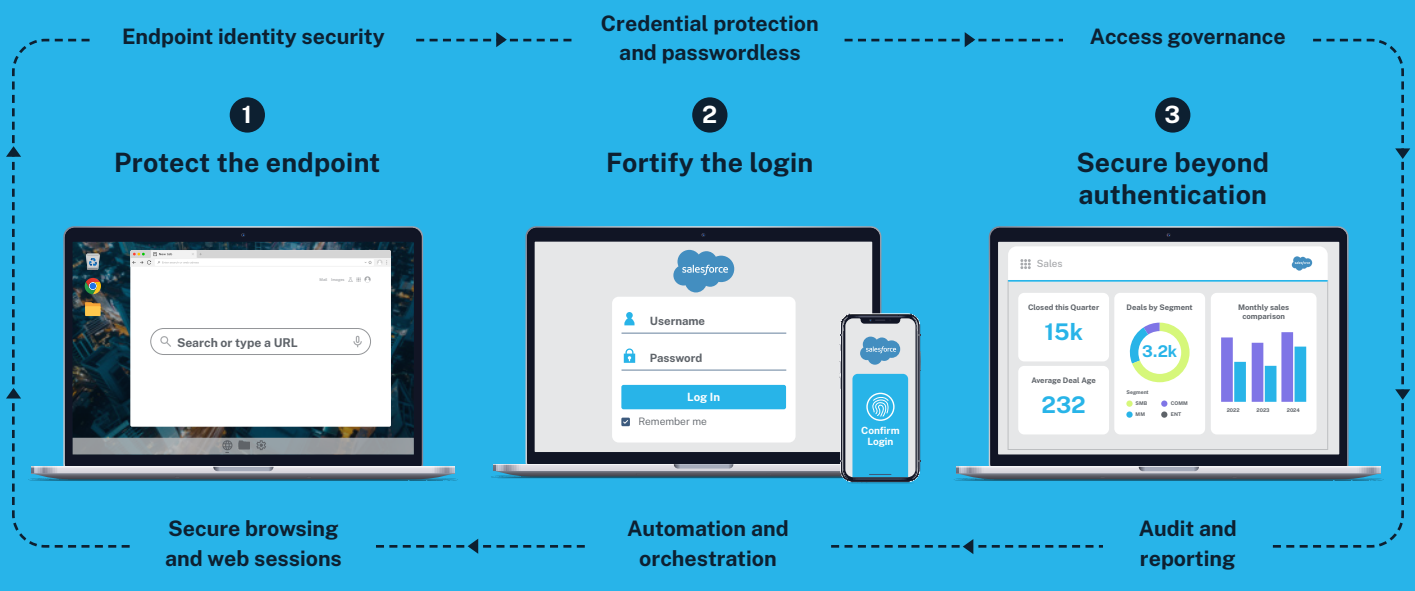
Managing user identities and access rights is a challenge for many information security organizations. Many rely on manually intensive, disjointed processes to onboard users and manage their evolving privileges — a time-consuming and error-prone approach that hinders IT service agility, squanders resources and is fraught with risk. It can take days or even weeks to grant new hires secure access to the tools they need to perform their jobs. And tracking and re-assigning user privileges across disparate applications and systems as people change roles is just as complicated. Threat actors can exploit mis-provisioned, overprivileged or orphaned accounts to launch attacks or steal data.

Use an identity lifecycle management solution to automatically onboard workers and manage their permissions throughout their tenure. Identity lifecycle management tools automate routine provisioning tasks, making it easy to add accounts and manage privileges as workers change roles and responsibilities. Most identity lifecycle management solutions support a wide variety of enterprise applications and services. Many integrate with HR and HCM systems to automate new-hire onboarding. And many include self-service capabilities and automated workflows to streamline permission request and approval processes and simplify change management. Lifecycle management solutions improve IT productivity by eliminating manual processes. They also reduce security vulnerabilities by eliminating over-permissioned and dormant accounts that can be exploited by internal or external threat actors.

CyberArk Workforce Identity Security

CyberArk Workforce Identity Security is designed to secure every worker's identity throughout their digital journey with the right level of access and privilege controls across all environments. The market-leading solution sets a new foundation for identity security by layering MFA, SSO and lifecycle automation with endpoint identity security, browser security, password protection and web session security to defend organizations against pre-authentication and post-authentication identity-based threats. The solution set includes advanced AI features and proven threat detection and response capabilities to ensure the digital journeys that users take day-to-day do not become attack pathways.

End-to-End Identity Protection for Your Workforce



Conclusion

Traditional perimeter-based security models and siloed access controls can't protect today's cloud-centric digital businesses. Identity has emerged as the new security perimeter and workforce user identities are a prime target for today's threat actors.

A unified, identity-first approach to securing workforce access can help you strengthen your security posture without compromising on productivity. The CyberArk Identity Security Platform built on the idea of securing every identity with the right levels of privilege controls employs a reimagined approach to workforce identity security to:

- Deliver measurable cyber risk reduction.
- Drive operational efficiencies.
- Enable digital transformation.
- Satisfy audit and compliance.

Next Steps

Learn more about securing the modern workforce in our buyer's guide: Selecting a Security-First Identity and Access Management Solution

To speak with a CyberArk team member about your organization's security needs contact us here.