Securing Your Workforce

CYBERARK

Protect the User Journey from Endpoint to Application

SOLUTION BRIEF

SOLUTION CAPABILITIES

- Provide your users with secure access to all the resources they need to do their jobs.
- Remove local admin rights at the endpoint and enforce least privilege.
- Enable a passwordless experience end to end.
- Automate on/offboarding and increase efficiency with user self-service.
- Securely manage and store passwords.
- Secure sensitive resources beyond the login with session monitoring.
- Review and certify access permissions to satisfy audit and compliance.
- Automate workflows across your identity infrastructure.
- Secure the web browser.

FedRAMP

fido CERTIFIED

Challenge

Securing the workforce is more critical than ever, as a single access misconfiguration or compromised credential can trigger a breach. Businesses face relentless identity-based attacks targeting employees, partners and vendors.

Managing access provisioning, password security, endpoint risks and compliance is complex, especially with a global workforce, remote employees and collaborators using unmanaged devices. In addition, balancing security with productivity remains a constant challenge.

Solution

CyberArk's Workforce Identity Security solution is designed for modern enterprises, prioritizing security without sacrificing productivity. It enhances traditional access management by embedding intelligent privilege controls™ throughout the workforce user's journey — securing identities from login to web session activity. The solution provides comprehensive security intelligence, robust automation and smart analytics, ensuring secure access to any resource, from any identity, on any device, and in any location.

To achieve a higher level of protection, CyberArk Workforce Identity Security offers the following capabilities:

Endpoint Identity Security

Endpoint identity security extends identity security and zero trust to workstations, securing all human identities. It enables organizations to discover and remove local admin rights, enforce role-based least privilege and detect identity-based threats. By reducing the endpoint attack surface and implementing application control, it mitigates credential-based attack paths, zero-day attacks, ransomware, and insider threats.

Secure and Adaptive Access for Every Identity to Any Resource

CyberArk Workforce Identity Security provides market-leading tools like single sign-on (SSO) and adaptive multi-factor authentication (MFA) to deliver secure, seamless access to cloud, mobile, SaaS and legacy applications. Powered by a robust user behavior analytics (UBA) engine, it enables organizations to create dynamic, risk-aware policies that adapt to changing contexts.

Password Management and Support for Your Passwordless Transformation

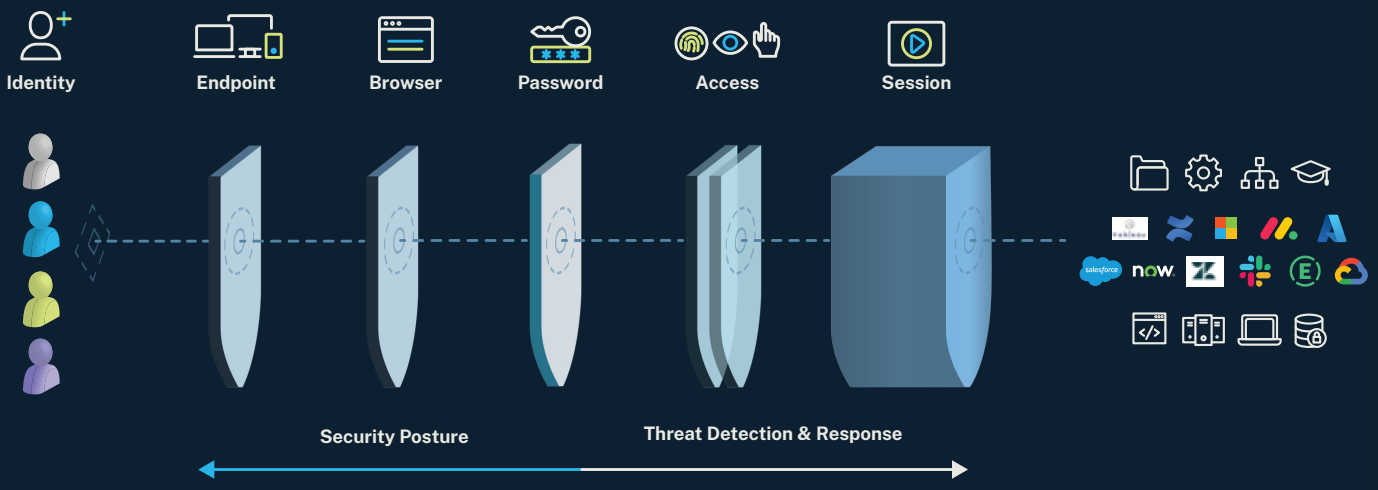
Compromised credentials remain a significant risk, even as the industry moves toward a passwordless future. CyberArk Workforce Identity Security secures user credentials through enterprise password management and passwordless workflows. CyberArk's password manager reduces password entry fatigue, enforces strong password hygiene and offers features like a compromised credential checker to prevent the reuse of stolen passwords. Organizations gain more control over how credentials are created, stored and shared.

CyberArk supports passwordless authentication across the entire user journey, from desktop login to federated access for native and SaaS applications. With flexible authentication options — including passkeys, OTP apps and FIDO2 authenticators — organizations achieve the right balance of security, usability and adaptability for their workforce.

Security Measures Beyond the Point of Login

While traditional access management tools are essential, they focus mainly on securing the login, leaving sensitive resources vulnerable during web sessions. CyberArk Workforce Identity Security provides visibility and control over user actions in high-risk sessions, allowing organizations to record sessions and generate detailed audit reports. With policy-driven controls to help prevent data leakage and trigger workflows based on user behavior, companies can enhance security, continuously authenticate and protect sensitive information throughout the session.

Protect Every Step of Your User's Journey from Endpoint to Application



Complete Browser Security

The web browser is a critical gateway to apps and cloud resources, making its security essential. While many organizations rely on consumer-focused browsers like Chrome, this approach creates security gaps and limits administrative control. The CyberArk Secure Browser is designed for enterprises, prioritizing both security and user experience. It helps prevent session takeovers and data leakage by protecting cookies, passwords and sensitive data.

CYBERARK®

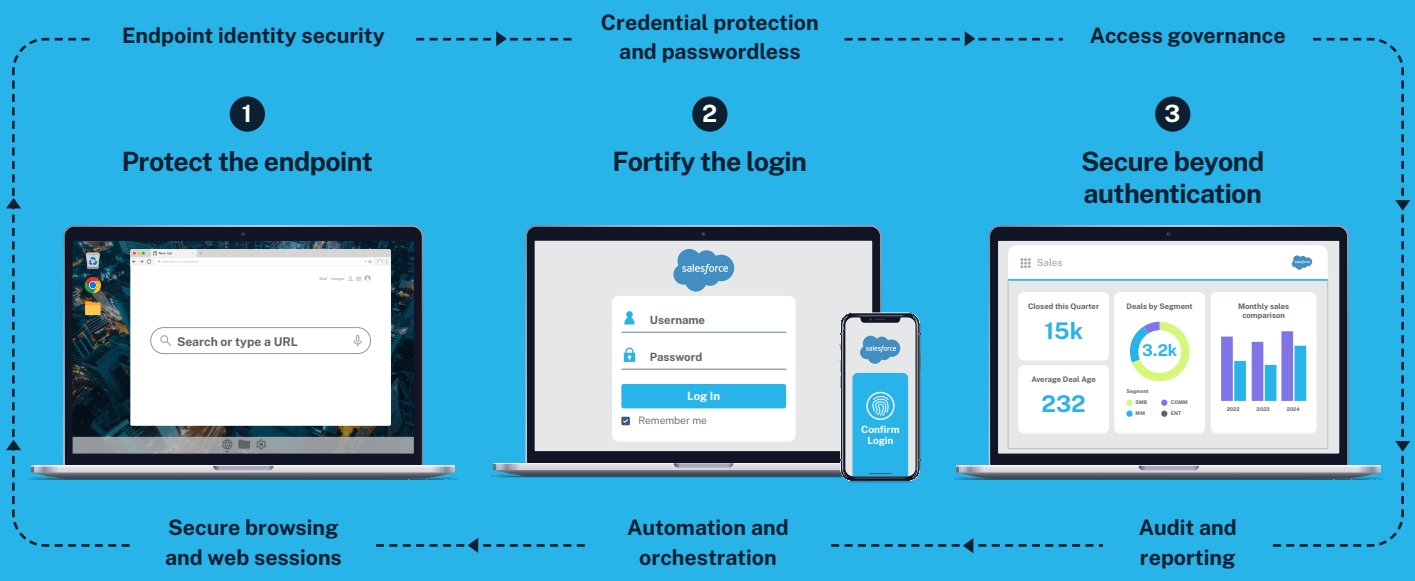
Centralized Governance to Enforce Compliance

After authentication, user actions within applications are constrained by roles, requiring organizations to maintain visibility and control throughout the identity journey. CyberArk extends session security to federated applications, enabling recording, auditing and protection of end-user activity. It enhances control for high-risk users through continuous access discovery, streamlined certifications, and comprehensive identity analytics, ensuring compliance post-access approval.

Smart Automation and No-code Workflows

Enterprises use smart automation to streamline user account creation, access permissions and self-service tasks like password resets throughout the identity lifecycle. By eliminating error-prone manual processes, organizations ensure a consistent, efficient approach to managing access requests, creating accounts, handling entitlements and revoking access when needed.

End-to-End Identity Protection for Your Workforce



CYBERARK®