CYBERARK®
THE IDENTITY SECURITY COMPANY®

eBook

Beyond the Login: Modern Identity Security for the Workforce

How to minimize risk with end-to-end protection across the entire user journey.

Table of Contents

Introduction

Traditional defenses have crumbled, leaving identity — the last standing perimeter of enterprise security — under constant attack. And with 94% of organizations having experienced an identity-related breach in the past year, the threat has never been greater.[1]

In the modern enterprise, the line between identity types continues to blur. Every user — no matter their function or the scope of their duties — can become an avenue for threat actors to exploit. This has made endpoint and user access the vehicle attackers frequently use to escalate privilege, disable security measures, compromise critical systems and exfiltrate sensitive data.

Traditional endpoint and access controls, such as endpoint detection and response (EDR), multi-factor authentication (MFA), single sign-on (SSO) and others, remain foundational but are no longer enough. Today, all workforce identities and their digital journeys must be secured end to end. As users interact with your internal systems, applications and data, it's important to protect every step — starting with the endpoint and initial login and continuing to what they access, when and how.

To make this a reality, enterprises need a holistic approach to intelligently secure endpoints, identities, access and privilege. But one-size-fits-all protections don't work in today's layered, constantly evolving threat landscape. And siloed, one-dimensional controls can't keep up in the long term.

It's time to reimagine workforce identity security.

This eBook will cover:

- **How the battle lines have been redrawn by changing work practices.**
- **Why an identity-first approach is essential for adequately securing workforce access.**
- **What the three pillars of modern workforce identity security are and their business impact.**

[1] CyberArk, "Identity Security Threat Landscape Report 2024," May 2024.

Endpoint and Identity: The Last Standing Perimeter

Nine in 10 organizations who suffered two or more identity-related breaches in the last year would agree: Securing workforce identities has never been more important.[2] Yet this is easier said than done.

Three factors play a role in why enterprises are finding it difficult to adequately secure workforce access:

1. Growing endpoint risks

The absence of a proactive, identity-centric approach to endpoint security leaves systems vulnerable to sophisticated threats. Existing security measures can be like an obstacle course for end users to overcome, hindering their workflows. While inefficiencies in compliance and audit processes exacerbate risk, they are marked by a lack of real-time visibility and control over endpoint security measures.

No wonder corporate-owned and managed workstations are a leading attack vector. And with remote working and bring-your-own-device (BYOD) programs now mainstream, this already significant attack surface has increased exponentially.

2. The evolution of workforce identities

Workforce used to mean only employees. Not anymore.

The average enterprise has become a complex web of internal and third-party users working on a mix of remote and in-office devices using cloud workflows and SaaS solutions. Contractors, partners and other external users need access to an organization's internal resources. And those third parties all have identities that need management and user journeys that must be secured.

3. The perils of privilege creep

Any identity can become privileged under certain circumstances.

Workforce identities navigate various levels of risk every day, making endpoint security, identity and access management moving targets. A workforce user may start off with access to their Windows or macOS workstation, native applications and some level of access to certain line-of-business (LOB) applications as part of their regular duties. However, as their responsibilities increase or they need access to more tools, their permissions will expand, creating a pathway to an organization's most valuable assets — and becoming an attacker's dream.

3x increase in identity and endpoint-related attacks

in the last year.[3]

71%

year-on-year increase in cyberattacks leveraging stolen or compromised credentials.[4]

91%

security leaders are concerned about third-party risks.[5]

84%

of identity stakeholders say security incidents have had a direct impact on the business.[6]

[2, 5] CyberArk, "Identity Security Threat Landscape Report 2024," May 2024.
[3] Verizon, "2024 Data Breach Investigations Report Executive Summary," 2024.
[4] IBM, "IBM X-Force Threat Intelligence Index 2024," February 2024.
[6] Identity Defined Security Alliance, "2024 Trends in Securing Digital Identities," 2024.

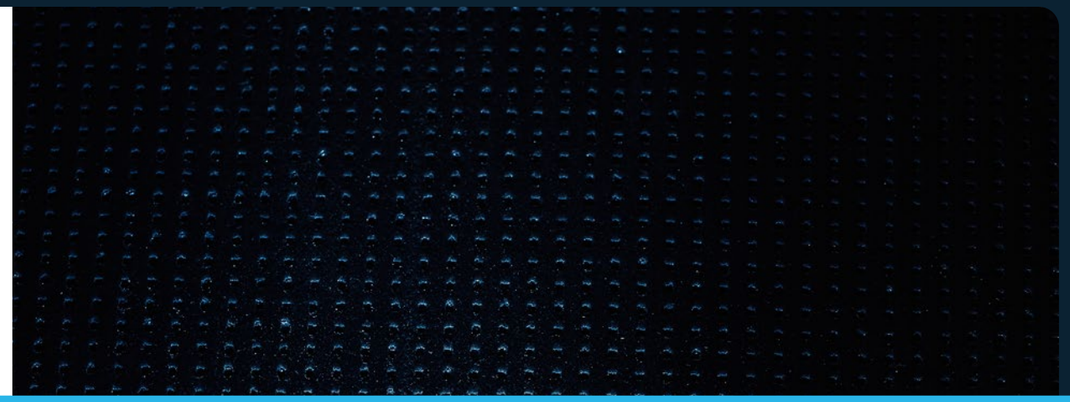
The Battle Lines Have Been Redrawn

Whether users are accessing high-risk SaaS platforms, general workforce SaaS applications or conducting personal tasks on a corporate machine, the primary entry point is often the web browser, and the vehicle for accessing all resources takes place on the user's endpoint.

If you consider how almost 60% of breaches are attributed to a combination of compromised credentials and exploitable vulnerabilities (from poorly protected web applications to associated threats like session abuse or cookie hijacking), this situation becomes increasingly worrisome.[7]

It's easy to see why workforce identities have become the new security battleground for the enterprise and why foundational endpoint and user access controls alone, such as MFA and SSO, are no longer enough. Although a necessity, these solutions act more like static checkpoints in the road. As standalone controls, they are outdated and unable to adapt to the diverse needs of today's workforce or the sophisticated tactics of modern attackers.

Instead, holistic end-to-end protection that secures the complete user journey and accounts for every attacker pathway — from the first mile of access at the endpoint to the last mile of data consumption via the browser — has become the new baseline for a successful defense.



While securing the inital login is crucial, it's just the starting point. Organizations need a strong layered approach, safeguarding the digital journey of every user at every step.

[7] Identity Defined Security Alliance, "2024 Trends in Securing Digital Identities," 2024.

The Need for an Identity-First Approach

In response to how the threat landscape is evolving, enterprises must find a way to secure workforce users' credentials, their browsers, sessions and the machines they work on, while dynamically governing access permissions.

To achieve this, security teams should start by adopting an identity-first approach to protecting enterprise systems from privilege misconfigurations, identity-based attacks and insider threats. By protecting workforce users and their digital journeys — from the initial endpoint login through to the last session interaction — they can prevent access pathways from becoming attack vectors.

This approach will allow the organization to link actions to specific users, giving security teams better visibility into user sessions. In turn, it will help with tracking and reviewing activity, identifying suspicious behavior and holding users accountable.

Securing Workforce Identities: The Six Key Requirements

It's also important to consider the user experience in this context. Enterprises must ensure that robust security measures do not impede user productivity or contribute to security fatigue.

The Hallmarks of an Identity-First Approach

Consistent

Leaning on centralized policies to consistently manage access across decentralized systems, ensuring access controls are uniformly applied to reduce the risk of privilege mismanagement.

Context-aware

Leveraging identity data and context (including location, time, device security status, etc.) to make dynamic, real-time decisions.

Continuous

Adapting controls throughout the user session and adjusting access rights in real time (for example, if a user moves to a new location).

The Need for an Identity-First Approach

The challenge lies in delivering seamless access while maintaining stringent security controls across the workforce, which can be distilled to six key requirements:

1. **Continuous endpoint identity security.** Enterprises must extend identity security to endpoints, instigating and fine-tuning privilege control policies based on user roles. Workforce users should be continuously authenticated and challenged for additional authentication where needed based on an active risk assessment.

2. **Credential protection and acceleration of passwordless authentication.** Stolen credentials continue to be the foremost cause of breaches, making passwordless authentication vital to reduce the attack surface and minimize friction. Many business applications still require a username and password at login, so it's vital that companies secure these credentials.

3. **Access governance.** Workforce users should only be given the permissions to perform their current role or task. Once completed, those privileges should be removed. This can be enhanced with the capability to evaluate real-time risk based on contextual factors.

4. **Controls that secure browsing and web sessions.** Enterprises must extend intelligent privilege controls to high-risk users, applications and sessions making sure every sensitive resource is protected with risk-appropriate controls beyond the point of login.

5. **Automation and orchestration.** To eliminate the risk of human error, improve efficiency and reduce costs, teams may want to automate their processes. By creating no-code workflows, companies can orchestrate onboarding and offboarding, for example, or respond to security alerts quicker.

6. **Strong audit and reporting.** Security teams must be able to continuously audit and enforce least privilege across the entire system (devices, applications, browsers and sessions) to ensure compliance.

End-to-End Identity Protection for Your Workforce

The New Foundation of Workforce Identity Security

Once an identity-first foundation has been established, enterprises must consider a defense in depth approach. This spans the three main pillars of modern workforce identity security:

1. Secure, seamless access
2. Intelligent privilege controls
3. Centralized management

Let's look at each pillar in turn and the actions to take secure the modern workforce.

Secure, Seamless Access

The first step is to streamline access to services, apps and resources from anywhere and on any device. This is the foundation of workforce identity security, providing a baseline of protection for all identities and endpoints.

Action: Start by enabling end-to-end passwordless access by layering SSO with adaptive MFA, setting the foundations for advanced authentication policies based on behavioral risk. From there, layer up to browser security, web session security and automated web session summaries that can enable security teams to monitor and audit end-user actions at scale.

Benefit: In addition to boosting productivity, seamless access boosts overall security posture by minimizing the risk of password and login fatigue, which can encourage workforce users to use insecure workarounds and weak recycled passwords.

Intelligent Privilege Controls

Workforce users engage with a variety of endpoints, data and applications as part of their daily tasks. They might handle sensitive information through high-risk endpoint native and SaaS applications, embodying a level of risk that fluctuates with their access privileges.

The blurring of the lines between identity roles compounds this issue. For example, it's not uncommon for employees to be given administrator rights to their machine and then be tasked with installing their own applications and managing security software — all while having sensitive access to systems and data through their browser. A single click can lead to endpoint compromise, credential and web session data theft and, ultimately, data exfiltration.

Action: To protect the enterprise, it's imperative to apply the principle of least privilege and dynamically adjust that privilege based on risk behavior through context-aware, real-time security controls. One of the most critical controls is an active defense of credentials and trust tokens scattered across the operating system, browser and third-party applications.

Benefit: Intelligent privilege controls provide granular, layered protection without increasing the burden on already-stretched security and IT teams. In turn, this curbs the inevitable risks of user's identity theft and privilege creep, providing deeper insights into identity-based threats and protections against both pre- and post-authentication attacks.

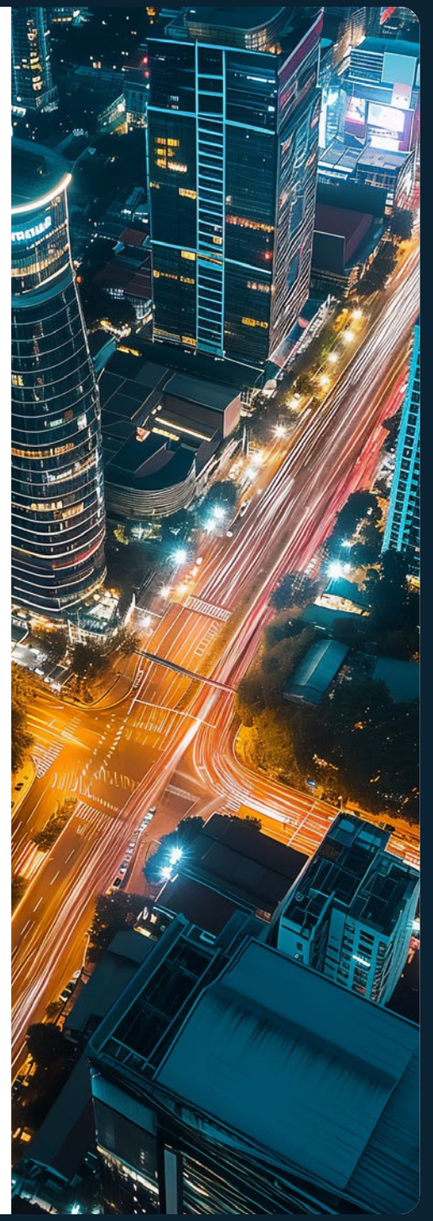
Centralized Management

Achieving secure, seamless access depends on a mindset shift when it comes to security management.

At present, nearly all (94%) security decision-makers rely on more than 10 vendors for identity-related cybersecurity initiatives.[8] However, given the limitations of siloed controls and the inherent visibility gaps this creates, modern workforce identity security depends on the introduction of a holistic, unified approach to managing and securing user journeys.

Action: Look for opportunities to consolidate controls and efforts to strengthen your overall security posture by fully integrating siloed solutions. Also, consider how a centralized management platform will allow you to automate smart flows throughout the entire identity lifecycle by using a single administration dashboard.

Benefit: Centralized management unlocks end-to-end visibility across the enterprise. In today's highly volatile IT environment where any user can become privileged, bringing centralized management to identity security will enable underlying solutions to share controls and collectively benefit from threat intelligence. As greater visibility means greater control, this approach also delivers enhanced risk mitigation for the organization while also enabling security teams to be more efficient.



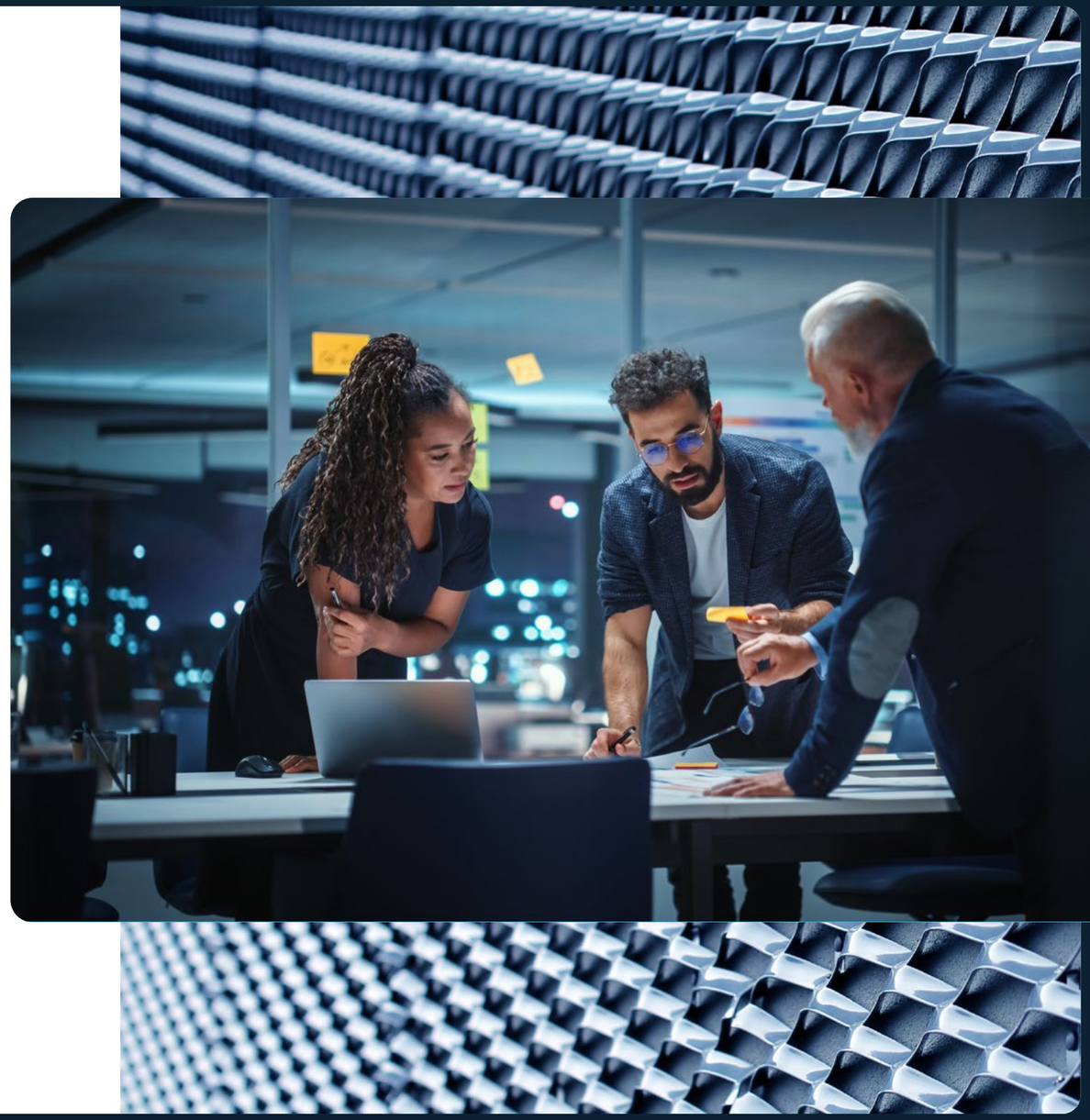
[8] CyberArk, "Identity Security Threat Landscape Report 2024," May 2024.

The Business Value of Workforce Identity Security

Adopting a modern framework for workforce identity security makes it so that compromise does not equal reward for bad actors.

By gaining visibility of all user journeys and implementing a blend of proactive and reactive controls, enterprises can better monitor, manage and audit access across workforce identities and enterprise resources.

The result is a significantly reduced attack surface which, in turn, minimizes the overall impact of security incidents — including brand and reputational damage that can have a long-term impact on the business.



Conclusion

The continued proliferation of identities — and the evolution of working patterns and threats — has put security teams on the defensive. Managing these challenges depends on taking a holistic approach to workforce identity security, one that protects user journeys end to end and across all potential attack pathways, while ensuring a frictionless user experience.

The CyberArk Workforce Identity Security platform achieves this balance. Built on the understanding that every user can be a privileged user, it empowers your workforce with easy and secure access while safeguarding against a growing number of sophisticated attack methods — meeting both today's needs and tomorrow's requirements.

Read the solution brief to learn more: Identity Security Built for Your Workforce.

About CyberArk

CyberArk (NASDAQ: CYBR) is the global leader in identity security. Centered on intelligent privilege controls, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud environments and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets. To learn more about CyberArk, visit https://www.cyberark.com, read the CyberArk blogs or follow on LinkedIn, X, Facebook or YouTube.