CYBERARK®

EBOOK

Identity Security: Why It Matters and Why Now

Remove Risk by Taking a Unified Approach to Managing Identities

Table of Contents

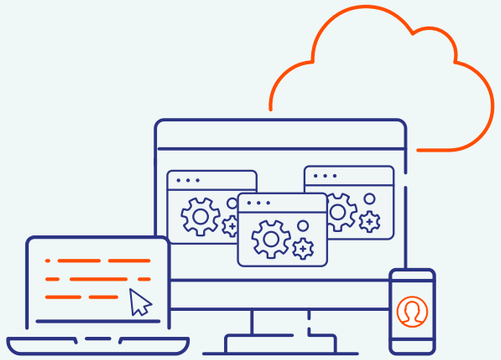
Introduction

The message from bad actors is loud and clear: Any identity is a target.

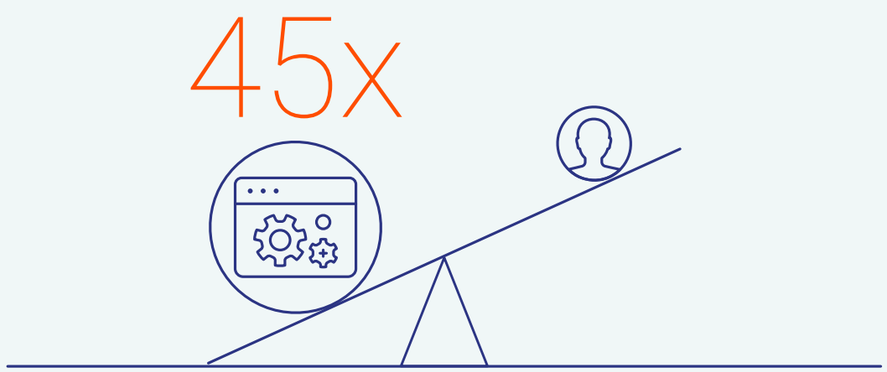
Looking at the modern enterprise landscape, it's easy to see why. Every employee has multiple identities and uses several devices. Third parties can access critical systems through their endpoint devices or apps. And that's before even thinking about the privileged access that machine identities need to function, or how they now outnumber their human counterparts 45 to 1.[1]

Identities are not inherently risky on their own, of course — so long as they are properly managed and secured. But enterprises' transformative initiatives — involving cloud migration, remote work, automation and DevOps — have resulted in a surge of identities with unprecedented access, making any identity a potentially high-value target. In multi-cloud environments, it's common for identities to be given a dangerous mix of entitlements, further extending the surface area that security teams need to protect.

[1] CyberArk 2022 Identity Security Threat Landscape Report, April 2022



The average staff member accesses more than 30 applications and accounts



Machine identities outnumber human identities by a factor of 45x

Source: CyberArk 2022 Identity Security Threat Landscape Report (n=1750)

Identity Proliferation: A Rising Threat

It should come as no surprise, then, that 80% of breaches start with compromised credentials.[2] IT and security pros are all too familiar with this, as well as the related issue of the explosion of identities created by organizations' digital transformation efforts. In addition, 98% of identity and security professionals said the growing number of identities are being driven by cloud adoption, third-party relationships and machine identities.[3]

But the management of identities can be at odds with digital transformation efforts. It's hard to strike the right balance between speed and security when the enterprise has become a complex web of physical and virtual endpoints, devices, cloud workflows and SaaS solutions.

Requiring users to repeatedly authenticate themselves to systems and applications — and to maintain multiple complex passwords — can become cumbersome and time-consuming. After all, things move quickly in this environment. But so do attackers, who still have the same modus operandi: to find an identity that has not been infused with intelligent privilege controls and exploit it for their own nefarious means. With more organizations accelerating to a hybrid or multi-cloud environment, there are even more gaps (read: identities) that attackers can use as entry points.

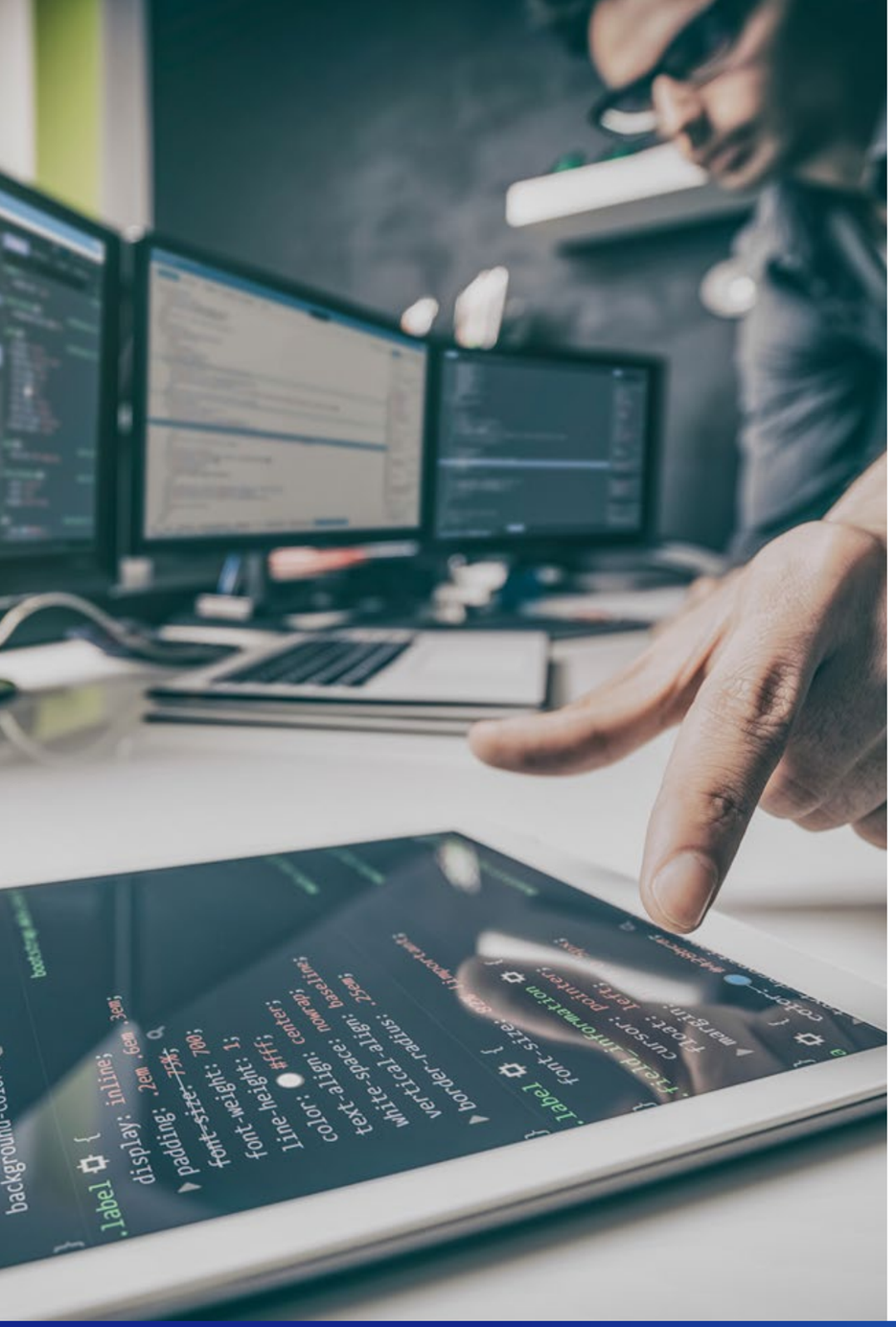
In short, enterprises are stuck between the proverbial rock (keeping all systems and data as secure as possible) and a hard place (keeping teams productive) — and bad actors are taking advantage.

[2] Verizon Data Breach Investigations Report, May 2022
[3] Identity Defined Security Alliance, 2022 Trends in Securing Digital Identities, June 2022

The Problem with Traditional Access Management Solutions

Identity has become the new battleground where enterprises are waging war against emerging threats as the attack surface becomes larger. But traditional identity and access management (IAM) solutions were not built as a defensive tool to manage the proliferation of identities that security teams now face — nor were they intended to be a vital security layer across the data center, hybrid, multi-cloud and SaaS environments.

Current methods to try and solve this problem only create more headaches. Organizations tend to use multiple tools to manage identities across the enterprise, leading to poor visibility. The more tools in the environment, the worse visibility gets — and the more siloed and fragmented things become. The result is a negative spiral impacting operational efficiency and creating vulnerabilities that open up the enterprise to threats.



All Roads Lead to Identity Security

It's not a question of whether an organization will suffer a cyberattack, it's when. The principles of "assume breach" and Zero Trust have risen as a way for enterprises to plug this gap and have become foundational to their security strategies. Identity Security is pivotal to securing identities and must meet the requirements of a successful Zero Trust implementation when it comes to identity-based risk management.

Embracing 'Assume Breach' and Zero Trust

As traditional network security barriers have dissolved, it's very likely your business has already been breached. If that's the case, the question is whether you're protected. In assuming that any identity across your organization – whether human or machine – may have been compromised, you should focus on identifying, isolating and stopping threats.

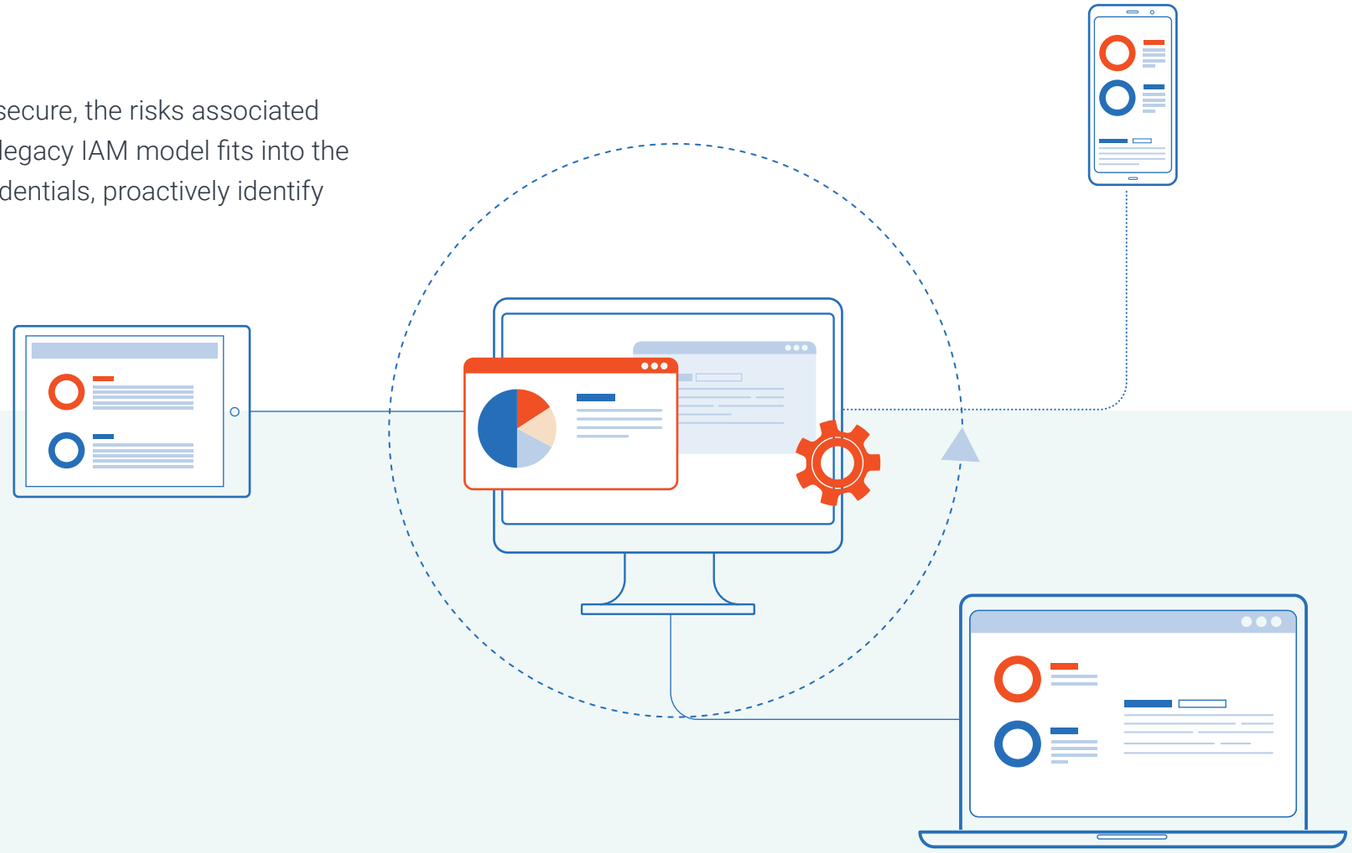
One of the foundational tenets of the Zero Trust architecture is to continuously authenticate and authorize all identities while securely granting just-in-time access with the right set of permissions.

A big part of the problem is that identity-driven attacks are hard to detect. Many organizations lack a reliable way to monitor suspicious user behavior to determine the signs of compromised identities. It was a more manageable shortcoming back when the network still had a perimeter. Today, since any identity — whether it's an IT administrator, third-party vendor, regular workforce user, customer account or machine — can become a digital attack path for bad actors, this lack of visibility is unacceptable.

Introducing Identity Security

As IT teams face an increasingly complex and disparate enterprise landscape to secure, the risks associated with identity compromise will only increase. Now is the time to rethink whether a legacy IAM model fits into the Identity Security mix. Enterprises need to layer in extra functionality to secure credentials, proactively identify threats and stop identity-driven attacks as they take place.

This requires a new definition for Identity Security.



What is Identity Security?

Centered on intelligent privilege controls, Identity Security seamlessly secures access for all identities and flexibly automates the identity lifecycle. This is paired with continuous threat detection and prevention – creating a unified approach.

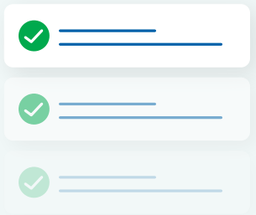
The Four Pillars of Identity Security

Seventy-two percent of executives agree that cybersecurity decisions made in the past 12 months have introduced new areas of vulnerability for the enterprise.[4] The potential to increase the attack landscape stems from identities accessing resources across various environments. It requires modern Identity Security to play a foundational role in any organization's strategy to protect against new and existing vulnerabilities.

Centered on intelligent privilege controls, Identity Security seamlessly secures access for all identities and flexibly automates the identity lifecycle, with continuous threat detection and protection — all with a unified approach. The main pillars of Identity Security are:

1 Seamless and secure access for all identities

All identities are granted just-in-time, just right, secure access to services, apps and resources when needed, from anywhere and on any device.



2 Intelligent privilege controls

Privileged access management (PAM) solutions underpin any Identity Security platform, providing intelligent controls to help secure credentials wherever they exist and enforce least privilege.

3 Flexible identity automation and orchestration

This pillar helps centrally secure and manage access for web services and embedded secrets used by applications, DevOps and automation tools throughout the lifecycle of every identity.

4 Continuous threat detection and protection

Detect identity threats on an ongoing basis and apply the appropriate Identity Security controls based on risk to enable Zero Trust.

[4] CyberArk 2022 Identity Security Threat Landscape Report, April 2022

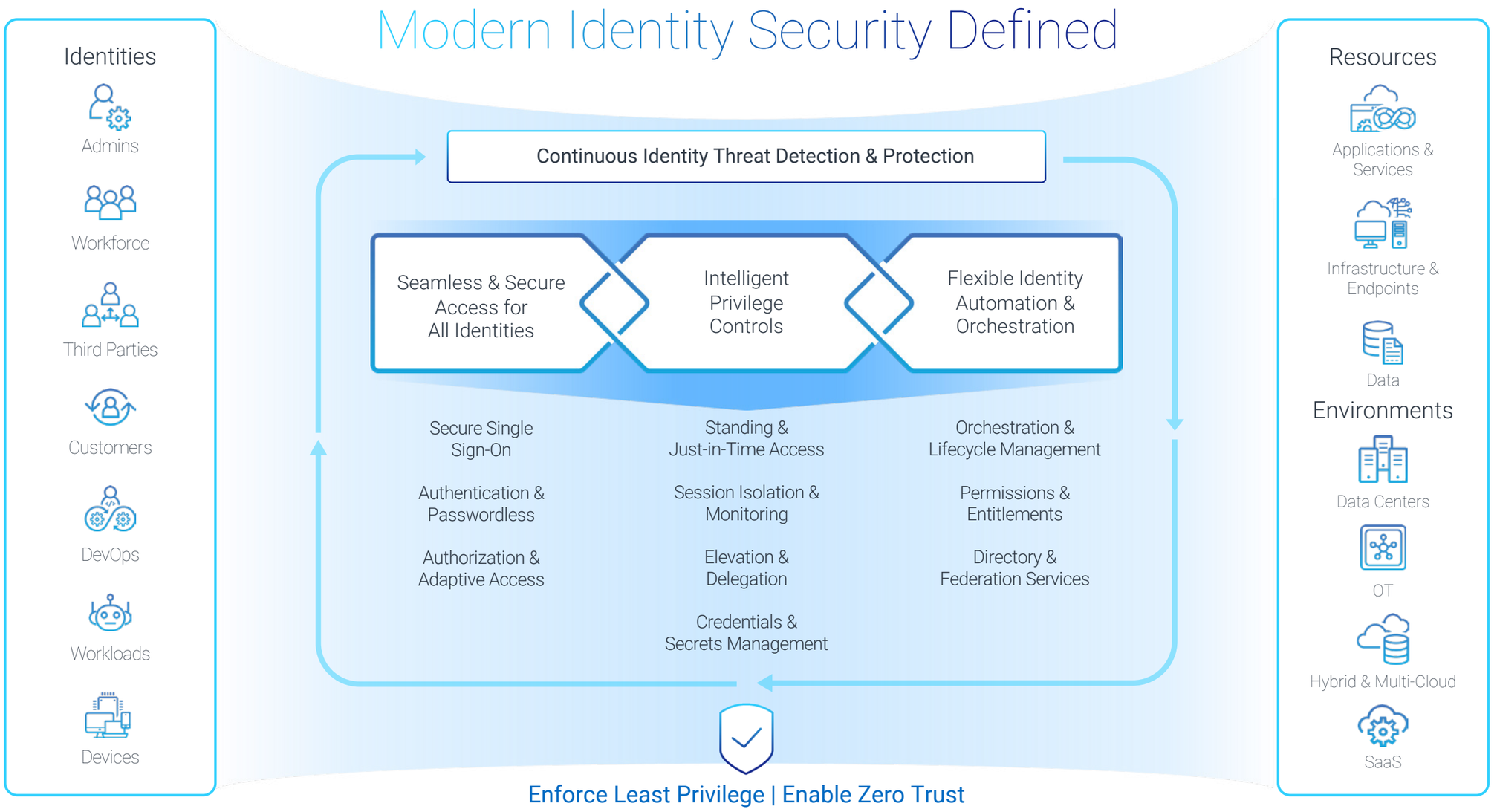


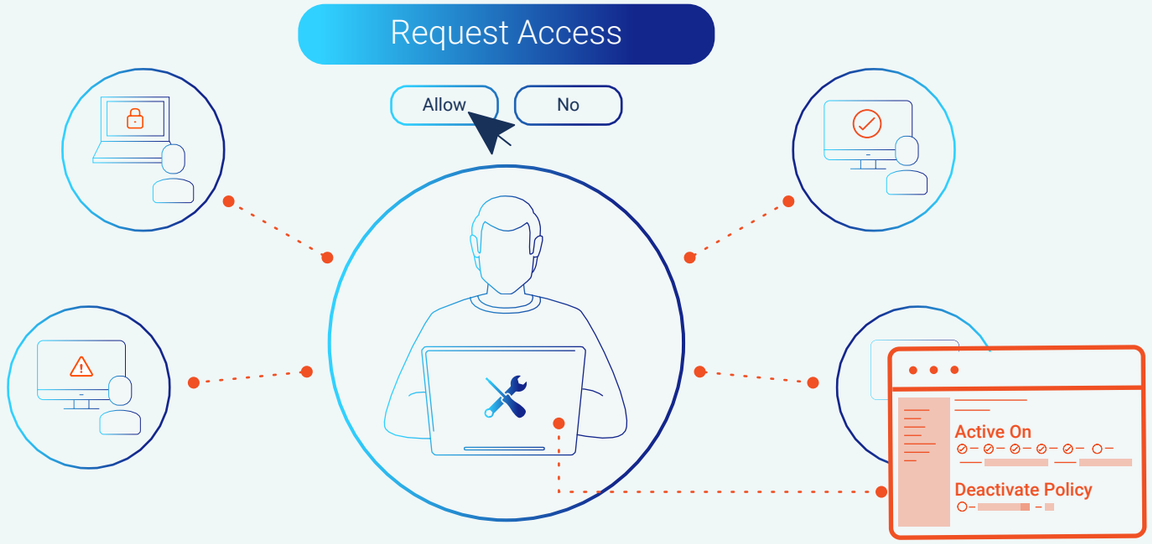
Figure 1 shows the capabilities as defined in a modern view of Identity Security.

Privilege Controls: The Heart of Identity Security

Privileged access management underpins the modern Identity Security framework. It provides the intelligent controls needed to secure any identities wherever they exist — not just those that the enterprise tracks as privileged accounts. This approach brings a robust security lens to secure human and machine identities accessing applications, infrastructures and data with continuous threat detection.

Intelligent privilege controls such as session isolation and monitoring, elevation and delegation are infused into access and identity management capabilities, including lifecycle management, permissions and secure single sign-on. This means access can be monitored on an ongoing basis across data center, hybrid, multi-cloud and SaaS environments, and intelligent Identity Security controls can be applied based on the risk profile of each identity.

As a result, just-in-time access becomes enabled across the board, and security teams can more readily identify, isolate and help stop harmful threats from compromised identities.



Identity Security Requirements

There are five foundational requirements for achieving the new approach to Identity Security:

1. **Discover all human and machine identities that have access to resources.** There must be centralized visibility across the entire enterprise estate to discover overprivileged identities, risky permissions and other unknown threats.

2. **Authenticate users with adaptive access based on context.** This step goes beyond a traditional IAM approach, helping to stop bad actors if they manage to compromise an identity.

3. **Use dynamic authorization, enforcing just-in-time access.** Identities should be given the right level of permissions needed to perform their roles, which should be removed when no longer required.

4. **Make the entire process secure to enhance security** without increasing friction that could impact the user experience and encourage risky behaviors.

5. **Conduct unified auditing across the entire enterprise landscape** to ensure everything is in order and to meet compliance.

The Business Value of Modern Identity Security

The risk of internal and external threats taking advantage of escalated privilege to access and exfiltrate critical data is a constant concern for security teams. The average cost of a data breach is $4.24 million[5] — but the impact of a successful cyberattack is not limited to the cost of recovery efforts and lost revenue. There will also be long-term brand and reputational damage, which can result in the business closing permanently.

Adopting a modern framework for Identity Security brings speed and security back into alignment. It gives organizations a holistic, risk-based approach to securing all identities and the peace of mind that their most critical assets are secure.

Business Benefits

1. **Drive operational efficiency:** Protect the enterprise by enabling just-in-time user access, removing the complexity associated with protecting identities at scale.
2. **Enable the digital business:** Expedite digital transformation efforts by delivering trusted experiences. Balance security with a frictionless user experience and efficiently adopt services across hybrid and multi-cloud environments.
3. **Reduce cyber risk:** Help prevent revenue loss, downtime and theft of critical data and IP by enforcing the principle of least privilege. If a breach occurs, that compromise is less likely to result in a reward for bad actors, minimizing the impact of security incidents.
4. **Satisfy audit and compliance:** One framework contains all audit and compliance requirements, offering greater visibility. This makes it easier to monitor, manage and audit across all identities (IT admins, remote workers, third-party vendors, etc.) and resources (apps and services, sensitive data, endpoints, etc.).

[5] IBM, Cost of a Data Breach Report 2021, July 2021

CyberArk Identity Security Platform

As the IT landscape gets more complex, enterprises need better ways to enable access while securing the business and defending against threats more effectively.

The CyberArk Identity Security Platform achieves this essential balance. It delivers on the requirements of a unified approach to Identity Security so that identities can access the right resources at the right times. The CyberArk Identity Security Platform drives operational efficiency — helping to keep attackers at bay while enabling the enterprise to drive key initiatives forward.

Key features include:

- **Empowerment of workforce identity:** Deliver simple and secure access to business resources using single sign-on and adaptive multi-factor authentication.
- **Real-time detection and prevention:** Ongoing and automatic monitoring, detection and threat mitigation enables enterprises to understand where they are exposed and take action.
- **End-to-end visibility:** A single admin portal provides visibility over the entire enterprise estate.
- **Secure privileged access:** Enterprises can discover and manage privileged accounts and credentials, eliminate excess cloud entitlements, isolate and monitor privileged sessions, and remediate risky activities across environments.
- **Central securing of application credentials:** All software and tools are secured by managing credentials.

Conclusion

With the proliferation of identities — both human and machine — IT security administrators face the challenge of containing identity sprawl as the attack surface continues to widen. Cybercriminals are taking advantage of the new entry points and exploiting organizations' weaknesses.

Helping to manage the surge in identities requires a modern approach to Identity Security that goes beyond the legacy model of identity and access management. It calls for a unified approach grounded in Zero Trust and least privilege.

As organizations look toward the future, there's a new standard to enable innovation and business transformation and reduce risk without compromise — and it starts with securing identities.

CyberArk is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads 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 www.cyberark.com, read the CyberArk blogs or follow us on Twitter via @CyberArk, LinkedIn or Facebook.

CYBERARK®