CYBERARK®
The Identity Security Company™

When Every Identity is at Risk, Where Do You Begin?

A Guide to Securing Workforce, Extended IT, Developer and Machine Identities

Table of Contents

Introduction

Today's threat landscape is defined by three realities that affect every organization's security:

1. New identities, proliferating to the point IT security teams expect 240% growth.[1]
2. New environments, extending from on-premises to hybrid and multi-cloud.
3. New attack methods including AI-fueled tactics.

Organizations once focused time and resources on protecting the most privileged of IT users. But now any identity can become privileged based on the resources it can access, including:

- IT staff, developers, vendors and workforce users collaborating in an ever-evolving hybrid model.
- Applications, bots and workflows operating behind the scenes to support cloud-based innovation.

These identities live in a constant cycle of accessing sensitive resources in critical environments — often guarded by easily compromised credentials and made riskier by excessive permissions.

As for your new environments: they present a paradox. By investing in hybrid and multi-cloud, the enterprise grows — and so does risk. While privileged identities perform tasks in the cloud, containers lie unprotected, standing privilege goes unchecked and secrets sit vulnerable in code.

Meanwhile, your organization isn't the only one innovating. Threat actors have a new arsenal of tactics and tools to breach organizations and launch attacks, including methods fueled by generative AI. They know that every identity at any access point is a gateway to an organization's most valuable resources.

For an organization to be secure, every identity needs the right level of intelligent privilege controls. In this piece, we'll share insights on today's threat landscape and how an integrated identity security approach can help you reduce risk, enable efficiency and protect everything your enterprise is building.

[1]CyberArk 2023 Identity Security Threat Landscape Report," 2023

New Identities

84% of organizations experienced an identity-related breach in the past year.[2]

New Environments

82% of IT leaders are adopting the hybrid cloud.[3]

New Attack Methods

9 in 10 IT security decision-makers expect AI to drive negative cybersecurity impact.[4]

[2]The Identity Defined Security Alliance, "2022 Trends in Securing Digital Identities," June 2022
[3]Cisco, "2022 Global Hybrid Cloud Trends Report," May 2022
[4]CyberArk 2023 Identity Security Threat Landscape Report," 2023

Securing a Threat Landscape Focused on Identities

Why should enterprises broaden their focus to secure all identities? Any compromised identity can be a gateway to the resources attackers target. But enterprises need a new approach to meet this challenge.

- 62% of IT security decision-makers say their organizations lack a complete picture of human and non-human access to sensitive resources.[5]
- 63% say their processes and technologies do not adequately secure the highest-sensitivity access for employees.[6]
- Meanwhile, their teams operate amid complexities such as staff and resource gaps, long hours and manual tasks.

As threats emerge, enterprises have deployed new tools ad-hoc to address them. Today, two-thirds use security tools from up to 40 different vendors.[7] But when solutions are bolted together, they're unable to:

- Share data on threats and act on insights; nor can they correlate alerts to find the signal in the noise.
- Apply an effective control for securing one type of identity (IT admin) to another identity (everyday employee).

It's no wonder that 60% of enterprises seek tighter integration between previously disparate security controls through vendor consolidation — while 65% view consolidation as a way to gain operational efficiencies.[8]

What can help you cut through these complexities? An integrated identity security approach, centered on applying intelligent privilege controls to all identities.

[5, 6, 7] "CyberArk 2023 Identity Security Threat Landscape Report," June 2023
[8] Enterprise Strategy Group, "Technology Perspectives from Cybersecurity Professionals," July 2022

An identity security approach, with AI and automation capabilities woven throughout, should be designed to:

- Extend intelligent privilege controls to all identities, ensuring they have only the right amount of access — and build these controls into the core of your strategy.
- Seamlessly secure all human and machine identities as they access critical assets and resources in environments including hybrid and multi-cloud, and from any device.
- Flexibly automate the identity lifecycle adding both security and simplicity to crucial areas like onboarding, provisioning, certifying and offboarding.
- Provide continuous threat detection and response, fueled by insights from user behavior analytics, third-party threat intelligence and more.

Securing a Threat Landscape Focused on Identities

Identity security is a strategy to enable Zero Trust and enforce least privilege. It requires a core set of technologies, people and processes that organizations need to secure the access of human and machine identities to their most critical assets and data across any environment or devices. Identity security controls are dynamic and adaptive in nature and ensure the right level of access is given based on risk.

Why apply intelligent privilege controls to any type of identity?

Because any identity can become privileged based on what it can access and the actions it can take.

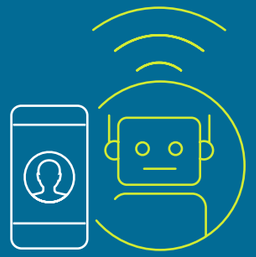
IT admin identities with high-risk access to critical infrastructure.

Identities of everyday employees with access to sensitive data such as customer information.

Identities of automated tools used by DevOps teams to build out cloud operations.

Built-in identities on endpoints and servers that attackers could use to steal data or install ransomware.

Machine identities built into Internet of Things (IoT) devices used by the workforce.



How to Secure Identities Across Three Key Areas

1. Identity Security for Developers and Non-human Identities

Developers often have more access than required — especially in lean times when rapid innovation is key to survival. Meanwhile, non-human credentials and identities integral to the DevOps world are widespread across enterprises, providing attackers with entry points. Non-human identities, such as applications, rely on secrets and other credentials to securely access sensitive resources, cloud workloads and other IT resources. But these secrets are highly vulnerable to attackers.

Ways to Reduce Risk

- Enable developers and security teams to secure, rotate, audit and manage secrets and other credentials.
- Extend intelligent privilege controls for credential management toward securing secrets for non-human identities in development environments.
- Help enterprises secure applications and automated processes, as well as integrate secrets management best practices into developer workflows.
- Centralize permissions management across AWS, Azure and GCP to implement least privilege.

Ways to Enable Efficiency

- Give security teams visibility and control of secrets across multiple cloud service provider accounts and native secrets manager instances, helping eliminate vault sprawl.
- Simplify how developers secure their code with a wide range of integrations.
- Avoid deployment delays for RPA and new apps due to security considerations.
- Centrally manage human identities so developers can securely access resources.

Spotlight: Protecting the Identities Behind Key Digital Initiatives

As enterprises deploy and accelerate developer-fueled innovation, 77% of IT security decision-makers say developers have too many privileges, making them highly attractive targets to attackers. In terms of non-human identities, only 25% say sensitive access to bots and robotic process automation (RPA) is secured.[9] Today's threats require an identity security approach built to protect every identity (human and machine) across every environment.

[9] "CyberArk 2023 Identity Security Threat Landscape Report," June 2023

How to Secure Identities Across Three Key Areas

2. Identity Security for Workforce Identities

More than half of employees have access to sensitive data[6], often via the rapidly increasing number of applications enterprises[7] deploy. The risk: easily compromised passwords to these applications are often the only thing standing between attackers and enterprise resources. Meanwhile, organizations lack visibility into the actions users take, and struggle with manual, time-consuming processes for managing identities.

Ways to Reduce Risk

- Validate users with context and risk-aware access controls, fueled by insights from user behavior analytics.
- Protect high-risk web applications sessions from insider threats and endpoint-originated attacks, through the intelligent privilege control of session monitoring and protection.
- Reduce the attack surface by eliminating password sprawl with SSO and enterprise-grade protection for employees' credentials for business applications.
- Ensure users only receive access to resources they need with flexible, automated provisioning workflows, using no- or low-code tools.

Ways to Enable Efficiency

- Improve user productivity by enabling streamlined access to apps and resources.
- Reduce IT workload with convenient self-service tools and passwordless authentication methods such as QR codes.
- Reduce IT complexity, delays, and errors with automated lifecycle management workflows, using no- or low-code tools.
- Improve security team's bandwidth through no-code app integrations and workflows.

[6,7] CyberArk 2023 Identity Security Threat Landscape Report," 2023

Spotlight: Intelligent Privilege Controls for Workforce Users Fueled by AI and Automation

Intelligent privilege controls, such as single sign-on, endpoint privilege management and secure web session recording, are at the core of an integrated identity security approach — especially as any identity can become privileged based on what it can access. In a unified platform, an enterprise can apply a risk-based approach to privilege controls for workforce users in SaaS applications, with auditing and reporting capabilities.

How to Secure Identities Across Three Key Areas

3. Identity Security for Highly Privileged IT Users

Even as a broader scope of identities gain sensitive access, a constant remains: IT runs on privilege. Enterprises rely on identities with powerful access rights to set up, maintain and run infrastructure and services powering digital initiatives. This includes IT admins but also key contributors to your cloud initiatives, from developers to site reliability engineers. Attackers who compromise privileged identities can move laterally, escalate privileges and then steal data, disrupt operations or deploy ransomware.

Ways to Reduce Risk

- Enforce zero standing privileges and enable just-in-time privileged access across hybrid and multi-cloud environments.
- Reduce risk of credential theft with risk-based credential management and rotation.
- Limit lateral movement with privileged session isolation and monitoring.
- Detect and respond to anomalous and risky behavior in privileged sessions.
- Protect against ransomware and credential theft with smart application control and risk-based credential and session management.
- Deploy foundational least privilege controls for workstations, servers and cloud environments.

Ways to Enable Efficiency

- Consistently and centrally analyze, secure, and monitor access across hybrid and multi-cloud environments.
- Improve audit and compliance review processes with informative data on user patterns and activities.
- Enhance IT and security teams' productivity with policy-based automation of endpoint privilege elevation.
- Quickly provision high-risk access with integrated PAM and Identity Management, leveraging automated workflows.
- Improve efficiency of vendor-led projects with just-in-time, Zero Trust access.

Spotlight: Securing Identities with AI-enabled Threat Analysis and Response

An integrated identity security approach should include a threat analysis service for workforce, IT and developer users. Enterprises can harness AI to automatically detect anomalous behavior that, on its own or in combination with privileged access misuse, could be a potential threat. Through this approach, IT security teams can receive real-time alerts that recommend response actions to expedite identification and analysis of high-risk events.

Understanding the Building Blocks of an Identity Security Approach

In an identity security approach, the underlying solutions are designed to share data, benefit from each other's controls and — similar to the people who are instrumental to making identity security work — collaborate. We've discussed a few key types of identities this approach can protect. Now let's explore additional components. Keep in mind, in an integrated framework, they do not stay in their lanes. For example, the world of intelligent privilege controls extends into non-privilege areas like workforce access.

1. Workforce and Customer Access

Ensure the right users have secure access to the right resources at the right times, by protecting workforce and customer credentials and tightly controlling access to on-premises and cloud-based applications, services and IT infrastructure.

2. Endpoint Privilege Security

Take control over unmanaged privilege on the endpoints to significantly reduce the area of attack and defend from threats by removing local admin rights, enforcing role-specific least privilege and improving audit readiness.

3. Privileged Access Management

Secure privileged credentials and secrets with comprehensive capabilities for operating systems, endpoints, cloud infrastructure and workloads, servers, databases, applications, hypervisors, network devices, security appliances and more.

4. Secrets Management

Secure and manage the secrets and credentials used by applications, machines and other non-human identities to access IT and other sensitive resources across both enterprise and external IT environments.

5. Cloud Security

Extend privilege controls to cloud environments by analyzing, securing and monitoring access. Discover and remove excessive permissions by visualizing access for human, machine and federated identities. Ensure zero standing privileges.

6. Identity Management

Automate the management of digital identities across enterprise IT environments and centrally create, maintain and analyze access to right-size permissions on the journey to least privilege.

Conclusion: Next Steps for Adopting Identity Security

You're protecting the enterprise at a time when three realities — new identities, new environments and new threats — are making the job more complex than ever. This dynamic calls for extending intelligent privilege controls to all identities, from IT users and everyday employees to developers and non-human identities.

An integrated identity security approach is the best line of defense against attacks in today's threat landscape, with a unified approach that enforces least privilege and enables Zero Trust. As you decide how to invest in your enterprise's security — and in turn, its ability to grow and compete — look for an identity security platform that is designed to enable these outcomes:

- Delivering measurable cyber risk reduction.
- Enabling operational efficiency.
- Securing key initiatives such as cloud migration and digital transformation.
- Satisfying audit and compliance.

As you work toward an identity security approach, it's important to remember: you don't have to do it all at once. You can start with your highest-priority focus area — such as privileged access management or cloud security — and build from there.

In addition, identity security is about more than technology. As you vet providers, ask about the people behind the solutions.

- Do they have an integrated team of threat researchers studying the latest attack methods?
- Do they have a red team that can evaluate and spot your vulnerabilities before attackers do?
- Do they have leadership that has been on the front lines of security and cyber warfare?

And like the platform you seek, does this team collaborate and continuously improve their offerings — to keep a step ahead of attacker innovation? This is how we approach identity security at CyberArk, with our customers' needs front and center.

About the CyberArk Identity Security Platform

Centered on intelligent privilege controls, the CyberArk Identity Security Platform seamlessly secures human and machine identities accessing workloads from hybrid to multi-cloud, and flexibly automates the identity lifecycle — all with continuous threat detection and prevention to enable Zero Trust and enforce least privilege. The platform is based on a set of foundational shared services, including AI-powered Identity Security Intelligence, that delivers a unified user experience through a single admin portal and enhances value with robust automation and analytics. Through our vast partner network and out-of-the-box integrations, CyberArk supports each organization along every step of their Identity Security journey, while helping them maximize existing security investments.

Read the CyberArk 2023 Identity Security Threat Landscape Report, our survey of 2,300 security decision-makers.

Read the Report

Speak to a CyberArk team member about your organization's security and business needs.

Contact Us

CyberArk 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 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®
The Identity Security Company™