CYBERARK®

The New Face of Identity and Access Management

How IT and security leaders can create a risk-based Identity Access Management (IAM) strategy to protect business and security priorities, together.

Table of Contents

The Perimeter has Evolved — It's Embedded in Every Identity

The world we know is redefined — as is how we secure it. When the pandemic emerged, your organization's IT and security teams were tasked with creating and securing an infrastructure for a distributed workforce, at a pace that felt like an overnight transformation.

Since then, you've been thrust into the driver's seat as urgent business priorities — such as the digitalization of your products and workflows — have created an explosion in the number of applications, and in turn identities, needed to execute on these initiatives.

7 Years

The pace at which companies have accelerated digital transformation initiatives, including their increased share of digital or digitally enabled products[1]

Each new door that opens to enable these identities to access your most important resources also represents new ways in for attackers. You know this. But you have to contend with an internal perception leading some to believe your organization's urgent need to drive the business forward is at odds with your need to protect it.

Nearly eight in 10 remote workers say their biggest hurdle is technology issues preventing them from connecting to corporate systems and resources.[2] With high-stakes projects on the line, employees feel compelled to problem solve productivity blockers, leading to shortcuts that attackers exploit, such as weak passwords.

With so much change happening at once, it will take more than traditional identity tools to be secure today. It takes a shared strategic vision between IT and security leaders built upon risk, innovative thinking and modern IAM capabilities to navigate access and security with speed, accuracy and peace of mind that your business is safe.

In this report, we explore key technological and cultural shifts and provide recommendations for what organizations can do to move fearlessly forward.

[1] How Covid-19 has pushed companies over the technology tipping point – and transformed business forever. McKinsey & Company. October 2020

[2] CyberArk State of Remote Work Study. December 2020.

We’re Living in a New World

Widespread shift to remote work across industries

According to the 2021 Gartner® CIO Survey, 64% of employees are now able to work from home, and two-fifths actually are working from home[3]

Embracing new ways of working

According to Gartner®, nearly 80 percent of workers are using collaboration tools for work in 2021, up from just over half of workers in 2019[4]

Explosion of nonhuman identities

Nonhuman identities are growing at 2x the rate of human identities across many organizations[5]

Identity: The Leading Attack Path

Attackers may be after your high-profile business assets, but they’ll go after any identity to make it happen — not only those of privileged users. All they need is a way in. Once inside, attackers employ more sophisticated ways to escalate their privileges and get what they need, from stealing customer data to holding operations ransom. In every case, these attacks can disrupt the flow of business and cost you dearly.

To protect the growing scope of identities attackers are targeting, organizations need to widen the security umbrella to cover new types of high-value users. This calls for a closer collaboration — and a jointly-created strategy built upon a shared vision — between security and IT leaders such as CISOs and CIOs.

The New Threat Landscape

61% of breaches stem from compromised credentials.[6]

613.5 Million passwords have been exposed in data breaches as attackers increasingly target end users.[7]

82% of people are somewhat or very concerned about increased security risks.[8]

70% of data and systems attacks involve IT and cloud infrastructure or personal data.[9]

97% of security leaders say credential theft attempts are on the rise.[10]

[3] Smarter with Gartner, "The Top 8 Security and Risk Trends We're Watching," Nov 15, 2021. GARTNER is registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.
[4] Gartner Press Release, "Gartner Survey Reveals a 44% Rise in Workers' Use of Collaboration Tools Since 2019," August 25, 2021.
[5] How to Secure and Govern Non-Human Identities. Forrester Webinar. February 2021
[6] 2021 Data Breach Investigations Report. Verizon.
[7] Have I been Pwned service. 2021
[8] 2021 Thales Access Management Index Report
[9,10] Ciso View Research Study. CyberArk 2021

IDENTITY-BASED PATHS FOR CYBER ATTACKS

The Unassuming Business User
After an Australian National University employee previewed a suspicious email, attackers breached the network and gained access to personal data, student records and tax file numbers.[11]

Misconfigured Access Privileges
NHS coronavirus contact-tracing app details were leaked after documents hosted in Google Drive were left open for anyone with a link to view.[12]

Sophisticated Supply Chain Attacks
In 2020, attackers found a back door into the Orion development pipeline. Once inside, they were able to infiltrate thousands of companies through a regularly scheduled software update.[13]

Approach IAM with the Future in Mind

In many cases, traditional Identity Access Management (IAM) solutions simply were not designed to secure modern enterprises that are in a continuous state of digital transformation. For businesses focused on innovation and staying one step ahead of trends, revisiting their existing IAM solution is an important, if exhausting, exercise. The good news is, you have options options that can provide a high level of protection, without interfering with your day-to-day operations.

Where We Were

- Network-based security
- Manual and tedious monolithic architecture
- Costly or missing audit and compliance capabilities

Network Based Security Perimeter

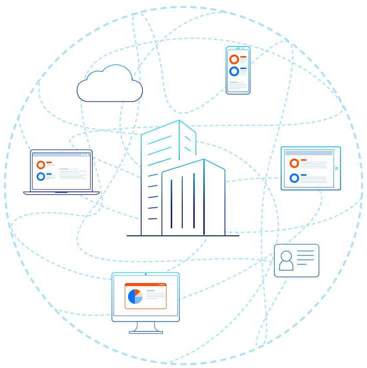
Application UI
Business Logic
Data Base

Monolithic and Manual Architecture

Where We Are

- Cloud-based, SaaS-delivered identity access management
- Security without boundaries
- Perimeter embedded into identities
- AI and machine learning to assess user behavior, gauge threats, lower risk and enable workforces

Security Without Boundaries



AI and Machine Learning to Identify Threats and Enable Workforce

[11] Inside a massive cyber hack that risks compromising leaders across the globe. Political reporter Stephanie Borys. ABC October 2019
[12] Secret NHS files reveal plans for coronavirus contact tracing app. Matt Burgess. Wired. 2020

A Comprehensive Approach to Security

A modern approach to Identity and Access Management can't be simplified to a single technology or tactic. And it can't stop at the initial point of access; user sessions within apps also present significant risk. Today's challenges call for a comprehensive approach and collaborative mindset across two key areas:

1. Building a CIO- and CISO-driven shared vision centered on risk
2. Executing on your vision, from fundamentals to innovation

Building a CIO- and CISO-driven Vision Centered on Risk

The philosophies of working securely and working efficiently seem less at odds every day. Organizations are seeing a correlation between an increase in digital initiatives such as cloud migrations and an increase in apps, identities and credentials. Your workforce is motivated, but one shortcut in the name of productivity can invite a breach that undermines everything they've worked to achieve.

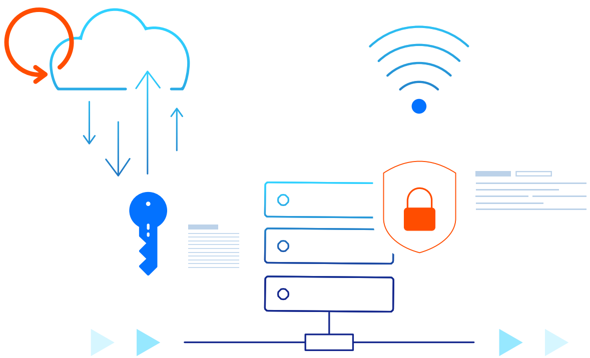
IAM has become more than just an IT issue — it affects both sides of the house — and can benefit from strong alignment and close collaboration. This is why alignment between the CISO and CIO is so essential in today's threat landscape. Partnering can put your organization in a position to protect and thrive.

With an IAM approach designed to both protect and empower the enterprise, developed in partnership between CISOs and CIOs, you'll be able to better identify where you have the most existing and emerging risk and put a risk-based security strategy in place to minimize threats.

THE CIO

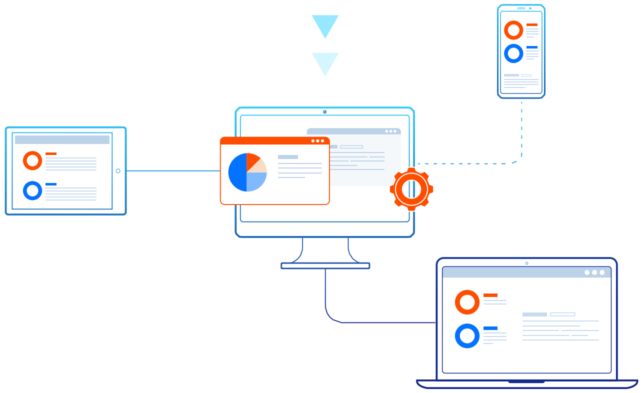
95% say their role is expanding[14]

- 64% into cybersecurity[15]
- 49% into data privacy/compliance[16]



THE CISO

- Focused on innovating to manage risk through investments
- 90% want to improve strategic alignment between security and business[17]



[14,15,16] 2020 State of the CIO Research Details the Expanding Roel of the CIO into the Customer Experience. CIO from IDG.

[17] The new CISO: Leading the strategic security organization. Khalid Kark. Taryn Aguas Deloitte. 2016. Review issue 19

1

2

3

Building a Shared Vision

Key steps to take and questions to ask
for IT and security leaders

STEP 1 | Develop a risk-based approach

- Across the organization, what's valuable, who has access to it and what high-risk actions can they take?
- As we roll out more apps and see identities increase, what are the chances of an attack, and what impact would it have?

STEP 2 | Set a clear strategy for IAM

STEP 3 | Ensure the right controls are in place to protect the right users

Executing on Your Vision, from Fundamentals to Innovation

Achieving your vision to reduce the greatest amount of risk and provide a frictionless user experience requires tools built for risk-based strategies. One important step you can take is ensuring your IAM solution is designed to secure high-value identities. Through this approach, you can track and secure all your high-value accounts, govern and control access, record and audit activity, and operationalize tasks. This allows you to protect a range of identities and workloads across different applications, systems, locations or devices.

At the fundamental level, a modern IAM solution designed for today's digital business should:

- ✓ Support legacy and existing systems
- ✓ Support digital transformation initiatives
- ✓ Work with modern services out of the box
- ✓ Enable operational efficiencies while reducing its overhead
- ✓ Above all, improve overall security posture

HOW CAN WE BALANCE THE NEED TO PROTECT OUR ORGANIZATION WITH THE NEED TO ENABLE THE BUSINESS TO THRIVE?

A collaborative approach will enable organizations to better identify and safeguard high-risk users like the below examples across three fields:

Financial Services
Users who have access to sensitive financial data and Personally Identifiable Information (PII) with the ability to take actions such as payroll changes.

Healthcare
Users with access to electronic healthcare records and patient billing data used in work environments such as shared workstations.

Marketing
Users with access to corporate social media accounts and other digital platforms for publishing content with shared credentials across team members

Using AI to outthink attackers

If bad actors are continuously adapting how they breach your organization, your IAM solution should be ever-evolving, too. Through machine learning and AI, you can manage more users, identify anomalous user behavior patterns and save time looking into false security alerts. Intelligent, adaptive capabilities can also help you tap into rich data, providing a holistic view of your enterprise. And most importantly, you can put that data to work to provide greater risk-reduction and a seamless user experience.

Align for Stronger Security

A risk-based approach, built upon a partnership of IT and security leaders, can provide a strong foundation for Identity and Access Management strategy. And when you leverage the right solution, you can:

- Identify and prioritize risks
- Reduce threats
- Prevent breaches and attacks
- Enable your business to thrive with speed and simplification

We recommend security-first IAM solutions and capabilities for multiple reasons. This approach enables you to protect a wider range of identities from any location or device, tap into rich data fueled by AI to grant access faster, and identify threats with greater accuracy and prioritization. Lastly, analytics paired with automation can help you evaluate and act upon insights on user behavior with the ability to adapt authentication standards and methods for any user scenario. Together, these capabilities will enable you to focus on the threats that matter most and keep your organization safe.

HOW ORGANIZATIONS CAN INNOVATE

Through machine learning and AI, discover more

- Autonomously evaluate user behavior and authentication activity
- Identify anomalous or high-risk security events
- Adapt its authentication methods accordingly

Through user behavior analytics, learn more

- Understand patterns in user behavior
- Visualize signs of emerging vulnerabilities
- Gain insight into actions high-risk users take

Through product and R&D innovation, do more

- Apply security and transparency to user activity in high-risk apps
- Secure and streamline credential sharing among teams
- Secure endpoints in an IT environment transformed for distributed workforces

The right partnership makes all the difference

No matter where you are in your journey, we're here to help. CyberArk is an established cybersecurity leader. Our leaders, product developers, R&D team and deep bench of threat researchers understand the pressures facing your company — and we're committed to helping you make sure your overall approach to Identity and Access Management is secure, sound and designed to enable success.

Learn more about CyberArk

CYBERARK®

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice. U.S., 02.22 Doc. TSK-809

THIS PUBLICATION IS FOR INFORMATIONAL PURPOSES ONLY AND IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER WHETHER EXPRESSED OR IMPLIED, INCLUDING WARRANTY OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, NON-INFRINGEMENT OR OTHERWISE. IN NO EVENT SHALL CYBERARK BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND IN PARTICULAR CYBERARK SHALL NOT BE LIABLE FOR DIRECT, SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE OR LOSS OF USE, COST OF REPLACEMENT GOODS, LOSS OR DAMAGE TO DATA ARISING FROM USE OF OR IN RELIANCE ON THIS PUBLICATION, EVEN IF CYBERARK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.