EBOOK

IDENTITY SECURITY: WHY IT MATTERS AND WHY NOW

FEARLESSLY **FORWARD.** ▶

CYBERARK®

TABLE OF CONTENTS

1 **HOW WE GOT HERE**

A look back at how the security perimeter disappeared.

2 **ALL ROADS LEAD TO IDENTITY**

Follow an attacker to understand why identity is the new battleground.

3 **THE IDENTITY PARADOX: SPEED VS. SECURITY**

Consider the challenges that come with protecting identities.

4 **ACHIEVE ZERO TRUST THROUGH IDENTITY SECURITY**

Understand the key elements of this modern approach to security.

5 **A ROADMAP FOR SUCCESS**

Kickstart your Identity Security strategy with a best-practice framework.

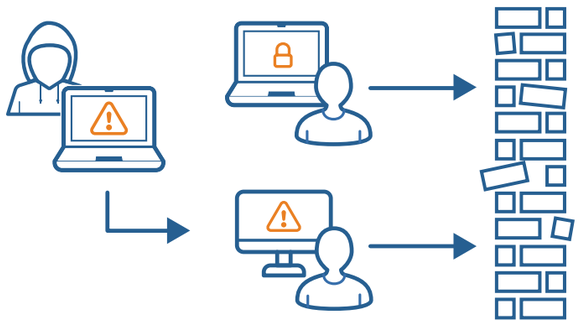
1 HOW WE GOT HERE

Security used to be simpler

It used to be that your employees worked primarily on site or connected through a VPN. They accessed your servers and applications, which were also on site, from corporate owned PCs. Fewer people needed access to critical business resources and, as long as you had built a strong security perimeter, the bad guys were kept out and your company was secure.

Digital transformation takes hold

To gain competitive advantage, companies began rapidly adopting cloud-based technologies and services, to deliver compelling digital experiences for their customers. We also witnessed increasing support for distributed workforces. These trends all accelerated tremendously in 2020 when only organizations with a strong digital business prospered.



The perimeter becomes obsolete

With digital innovation came newfound technologies and users, putting increasing strain on the integrity of perimeter-based security approaches. Each and every customer, remote worker, device and application now potentially needed an entry point to your most sensitive systems. Topping it off, we entered a worldwide pandemic and, in an instant, had to scramble to connect home offices, support new devices and bring new collaboration tools online as quickly as possible. With thousands of entry points, your network perimeter became even more porous and cyber attackers knew it.

Number of Attacks Exploded

400%

Rise in Reported Cyber Attacks

FBI, April 2020

667%

Rise in Spear-phishing Attacks

Barracuda, March 2020

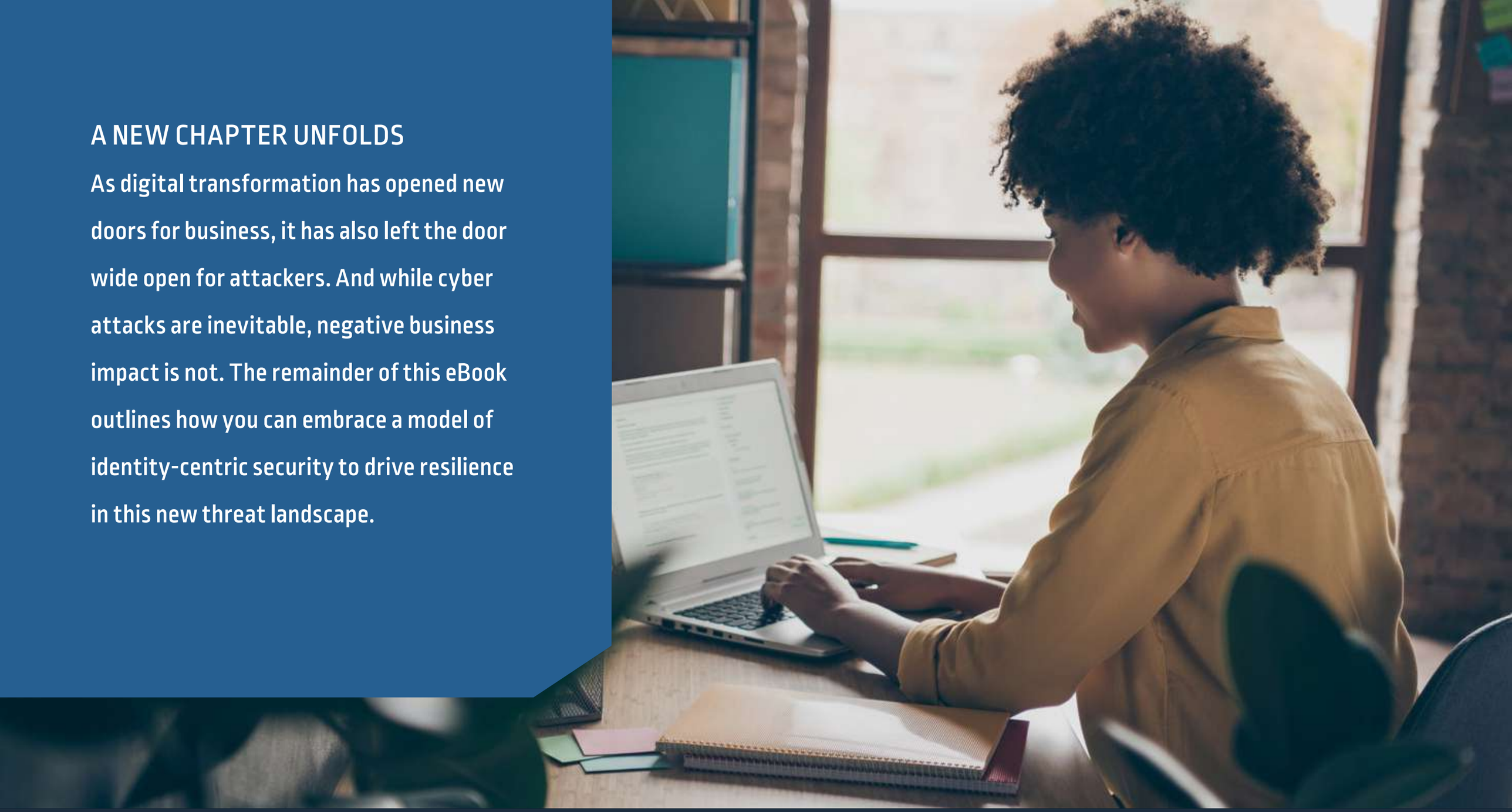
800%

Rise in Ransomware Attacks

MonsterCloud, August 2020

A NEW CHAPTER UNFOLDS

As digital transformation has opened new doors for business, it has also left the door wide open for attackers. And while cyber attacks are inevitable, negative business impact is not. The remainder of this eBook outlines how you can embrace a model of identity-centric security to drive resilience in this new threat landscape.



2 ALL ROADS LEAD TO IDENTITY

In today's hybrid and multi-cloud world, identity is the new security perimeter. Traditional network security barriers are no longer enough, and all identities can be an attack path to an organization's most valuable assets.

Any Identity

- ✓ IT Admins
- ✓ Employees
- ✓ Vendors
- ✓ Customers
- ✓ Machine Identities

Securing the expanding number and types of identities – within business applications, from hybrid to multicloud workloads and throughout the Dev/Ops pipeline – requires a new approach rooted in privileged access.

79%

of enterprises have had an identity-related breach within the past two years

December, 2019. The State of Identity: How Security Teams are Addressing Risk

ANATOMY OF AN IDENTITY-BASED ATTACK

Step 1: Acquire a valid set of credentials for an identity, any identity.

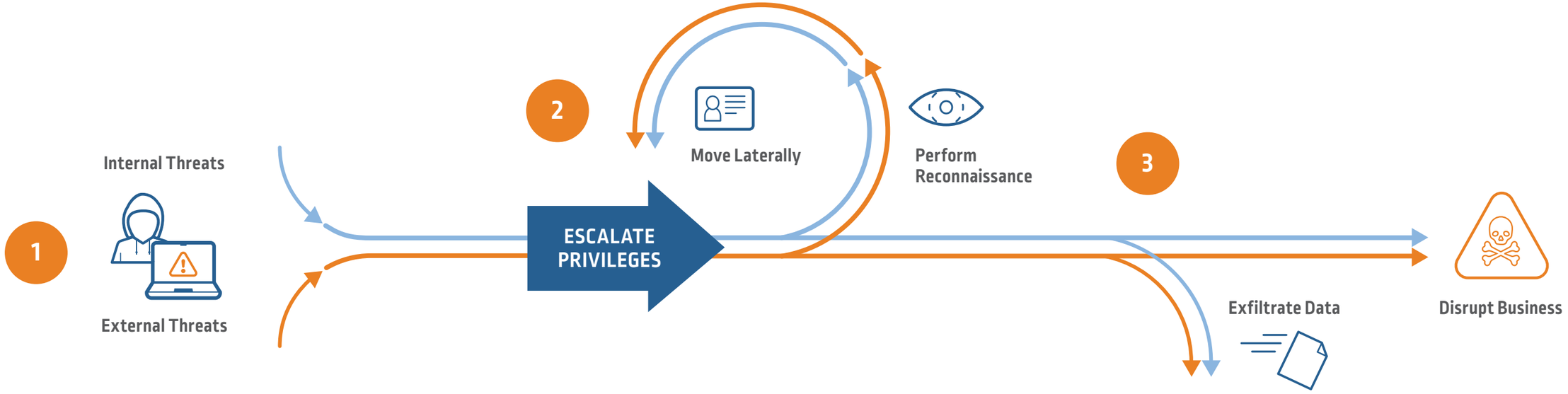
There are many methods attackers use to establish an initial entry point but compromising identities is an especially productive tactic. One of the most effective is phishing or social engineering that tricks employees into leaking usernames and passwords. Also topping this list: insider threats and unsecure application code where credentials are hard-coded and unintentionally exposed to attackers.

Step 2: Move laterally and vertically to escalate privilege.

With this newfound access, attackers start to worm in deeper, moving between identities, applications and systems to uncover new levels of access. Privileges are escalated higher and higher until the attackers reach the ultimate prize: systems, applications and databases containing critical business assets such as your customer data and sensitive intellectual property.

Step 3: Attack.

With high levels of privileged access in hand, attackers begin to exfiltrate your critical customer, financial data or intellectual property. Or, as we increasingly see in the headlines, attackers threaten to shut down systems or leak sensitive data unless a ransom is received. Either way, the outcome is the same: expensive and painful remediation that consumes cycles of security teams that were already stretched to the limit to begin with.



EMBRACING AN “ASSUME BREACH” MENTALITY

With traditional network security barriers dissolving, it is very likely your business has already been breached. The question becomes, are you protected even if that’s the case? This is the premise of a Zero Trust approach, which we will discuss more in chapter 4. By assuming that any identity – whether human or machine – in your network may have been compromised, you can turn your attention to identifying, isolating and stopping threats from compromising identities and gaining privilege, before they can do harm.

3 THE IDENTITY PARADOX: SPEED VS. SECURITY

As the pace of digital continues to accelerate, security strategies can only be effective if they are balanced with needs of the business to move quickly and operate unencumbered.

Requiring users to repeatedly authenticate themselves to systems and applications – and maintain multiple complex passwords – is cumbersome and time consuming. At best, IT teams spend an unacceptable amount of time dealing with password resets, account lockouts and provisioning users with new software and tools. At worst, workers develop clever ways to get around the controls you worked hard to put in place — or avoid using company approved systems and applications altogether.

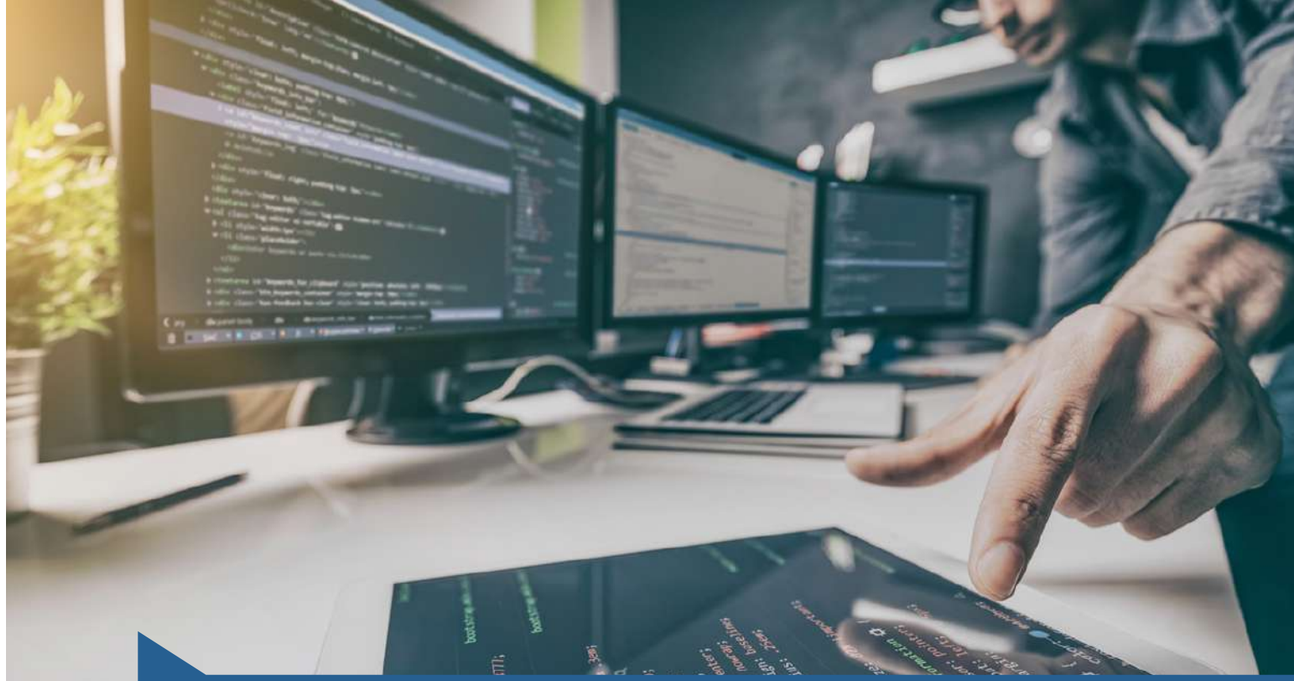
In short, businesses find themselves stuck between a rock (keeping all systems and data as secure as possible) and a hard place (keeping teams productive). There is a huge need for solutions that can strike a balance. One that empowers users by giving them fast, responsive and easy access to everything they need, but does so in a way that is continuously secure and keeps attackers at bay.

> **"Speed is the new currency of business."**
>
> *Marc R. Benioff,*
> *Chairman and CEO, Salesforce*

Striking a balance in the DevOps pipeline

Embracing digital innovation also means embracing DevOps, where developers and IT teams rely heavily on automation and cloud services to accelerate the pace of innovation and software releases. But securing that pipeline is often inconsistent. Often, teams hard code privileged credentials directly into code, rely on native security components of the tools or sometimes don't prioritize security at all. Not always because they don't want to but also because they don't understand the specific security needs.

As a result, the credentials and secrets used by application and machine identities become easy targets for attackers. And because security isn't typically addressed until the end of the process, developers feel the pain in terms of last-minute code changes and delayed releases.



> **"Think in terms of, "How do I allow my developers to do the right thing without stifling their agility?"**
>
> *Fred Gibbins, Senior Vice President and Chief Information Security Officer, American Express Company*

4 ACHIEVE ZERO TRUST THROUGH IDENTITY SECURITY

While traditional perimeter-based security relies on trying to separate the bad guys from the good guys and assumes that systems and traffic within the data center can be trusted, Zero Trust assumes that the bad guys are already in your network and have access to your applications and systems.

In a Zero Trust model, every identity is authenticated and authorized before granting access.

Verify every user

Validate every device

Intelligently limit privileged access

Zero Trust is not a single technology but an approach that ensures every user's identity is verified, their devices are validated and their access is intelligently limited to just what they need – and taken away when they don't.

Identity Security offers a set of technologies that are foundational to a Zero Trust approach. The Identity Defined Security Alliance provides a **useful framework** for understanding the technology components – from devices to network, applications and storage – that require protection at the identity level.

Coupled with proper shifts in people and process, Identity Security offers the promise to finally resolve the battle between security and business agility.

71%

Made organizational changes to the ownership of identity management

December, 2019. The State of Identity: How Security Teams are Addressing Risk

IDENTITY SECURITY DEFINED

Identity Security focuses on securing individual identities throughout the cycle of accessing critical assets. This means **authenticating** that identity accurately, **authorizing** that identity with the proper permissions, and providing access for that identity to privileged assets in a structured manner – all in a way that can be **audited** (or accounted for) to ensure the entire process is sound.

STRONG AUTHENTICATION

- Contextual, risk-based and adaptive access management (SSO, MFA, LCM)
- Strong passwordless authentication factors including biometric, mobile push and USB tokens

CONTEXTUAL AUTHORIZATION

- Secure privileged access for human users, applications and other non-human identities
- Least privilege and just-in-time access principles enforced across all platforms, endpoints and applications

FRICTIONLESS ACCESS

- A single pane-of-glass to administer, provision, enable access and secure all identities and resource types
- Automated workflows and self-service (e.g., app access, user provisioning, account and password reset)

AUDIT AND ACCOUNTABILITY

- Secure brokered sessions to ensure accountability, monitor/identify risk and produce tamper-proof audit trails
- Risk analytics to monitor access activity and act on suspicious behavior in real-time

SEAMLESS INTEGRATION

- Seamless integration with your existing technology stack including third-party threat intelligence and DevOps tools
- Strong developer support through APIs, SDKs and tutorials

5 A ROADMAP FOR SUCCESS

Identity Security offers organizations the peace of mind that their most critical assets are secure while accelerating business agility. But getting started can be half the battle.

The CyberArk Blueprint is a best practice framework for identity security success. It prescribes identity security controls and best practices for organizations using conventional on-premises infrastructure and software development methods, as well as for organizations embarking on digital transformation projects. Organizations use the Blueprint to identify and address their greatest identity security risks as quickly as possible, while also building a future-proof identity security program.

Founded on incident response lessons learned and cutting-edge research from the CyberArk Labs team, the Blueprint provides vendor-agnostic and measurable risk-based advice to defend against identity-based attacks.

Chart your course with the CyberArk Blueprint

Request your complimentary assessment

Cyberark.com/blueprint

U.S., 02.21

CYBERARK®