LEARNING MADE EASY

CyberArk Special Edition

Identity Security

for dummies®
A Wiley Brand

Defend against attacks

Enable digital business and drive efficiency

Satisfy audit and compliance

Brought to you by

CYBERARK®

Aaron Pritz

About CyberArk

CyberArk is a global leader in Identity Security. Centered on privileged access management, CyberArk provides a comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, and hybrid cloud workloads and throughout the DevOps life cycle. CyberArk is a public company trusted by more than 6,900 of the world's leading organizations to help secure their most critical assets. These companies include more than 50 percent of the Fortune 100 and more than 35 percent of the Global 2000 in 110 countries.

To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blogs, or follow on social media:

Twitter

LinkedIn

Facebook

Identity Security

CyberArk Special Edition

by Aaron Pritz

for dummies®
A Wiley Brand

Identity Security For Dummies®, CyberArk Special Edition

Published by **John Wiley & Sons, Inc.,** 111 River St., Hoboken, NJ 07030-5774, www.wiley.com

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN: 978-1-119-83057-3 (pbk); ISBN: 978-1-119-83060-3 (ebk). Some blank pages in the print version may not be included in the ePDF version.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Manager and Development Editor: Carrie Burchfield-Leighton

Sr. Managing Editor: Rev Mengle

Acquisitions Editor: Ashley Coffey

Business Development Representative: Molly Daugherty

Production Editor: Mohammed Zafar Ali

Table of Contents

Introduction

For centuries, thieves, con artists, hackers, malicious insiders, and pretty much all forms of bad actors have relied on taking on the identity of another person to achieve their impact or goal. In fact, in the article "10 of History's Greatest Con Artists" by Fodor's Travel, you can find stories of how infamous imposters deceived others out of money, control of computer networks, and other valuable treasures. (Check out `www.fodors.com/news/photos/10-of-historys-greatest-con-artists` for the full history lesson.)

For organizations (companies, non-profits, schools, governments, and so on), an "identity" describes who someone or something is. Identities can include customers, partners, employees, or other stakeholders within the organization that have various levels of access to computers, networks, cloud applications, smartphones, routers, servers, controllers, sensors, and more. Identities are also non-human as organizations digitally transform their operations and automate more processes.

Within organizations, companies have often treated Identity and Access Management (IAM), Privileged Access Management (PAM), and other protective control areas like Multifactor Authentication (MFA) across separate teams or even divisions of the company. With the company "perimeter" shifting from the need to protect the internal network to securing remote workers and external cloud services, the game has changed.

A holistic focus on Identity Security, which is a comprehensive solution for securing all identities used in an organization, is necessary to secure modern companies and the foundation of Zero Trust security strategies. With this focus, you can help your organization protect identities and ultimately safeguard the company.

About This Book

This book is written with the expectation that anyone in your company should be able to read it, understand the content, and be armed with the knowledge to better articulate the need for Identity Security. Often, cybersecurity books go into significant

technical depth that's great for security engineering, software developers, and architects. But you can expect this book to be conversational, with plenty of examples, analogies, and elements designed to make this security topic more approachable.

Icons Used in This Book

Throughout this book, I use special icons to call attention to important information. Here's what to expect:

This icon points out information that are key things to remember as you translate your learning into action.

These sections may dip a bit deeper into the technology pool, but don't worry; I made sure the deep end isn't over your head.

Tips are nuggets of information you may want to apply as you evolve your skills and your Identity Security program.

Nobody likes pit falls, so watch out for these. Warnings are lessons learned from experience so you can avoid and save yourself from costly mistakes.

Beyond the Book

It's my hope that this book gives you a better understanding of Identity Security and how to think about it holistically at your company. If you're left wanting more, visit the CyberArk website at `www.cyberark.com` where you can learn more about these concepts and platforms to achieve these concepts effectively.

IN THIS CHAPTER

- Looking at the four As of Identity Security
- Defining Identity Security's place at the center of security
- Integrating Identity Security and cybersecurity

Chapter 1
Defining Identity Security

Identity Security is a recently emerged strategy that encompasses the technology, people, and processes needed to secure identities against attacks. Identity Security assumes that any identity — whether IT admin, remote worker, third-party vendor, device, or application — can become the entry point that an attacker uses to gain access a to a company's most valuable assets. The attacker does this by stealing identities and credentials and exploiting other vulnerabilities in the network to gain increasingly higher-level access, creating an attack path to high-value targets within the organization.

In this chapter, you discover the basics of Identity Security, how Identity Security could be the central focal point of a company's security approach, and how Identity Security and cybersecurity projects, programs, and teams can work better together.

The Four As of Identity Security

Identity Security follows a Zero Trust model. The Zero Trust model originated as early as 1994. It has been re-popularized over the years by both practitioners and marketers, sometimes with very different intentions and levels of understanding. At its simplest form, the Zero Trust model suggests that devices and identities shouldn't be trusted by default, even if they're connected to a managed (and "secure") corporate network. They also shouldn't be trusted just because they were previously verified.

This level of security has become critically important and became much more apparent when the COVID-19 pandemic hit in 2020. Companies were forced to shut down physical offices and immediately enable employees to work remotely as business. Workloads and data moved to the public cloud and the use of Software as a Service (SaaS) exploded. These employees and systems needed remote access to resources that were previously secured by a corporate network, which no longer works as an effective strategy for security. By implementing an Identity Security strategy, businesses can protect their high-value assets while allowing identity-based access to the resources necessary for the business to function.

REMEMBER

The basic concepts of Identity Security rely on the four As of Identity Security:

- **Authentication:** Authenticate every identity accurately. Is this person/user/device/bot/script/account really who or what it's claiming to be? This identity could be a legitimate company employee, hacker, application, or automation tool. The only way to know is to have a system and/or process that accurately authenticates the identity. After an identity is authenticated, it doesn't get a free pass to access the system with impunity. In certain cases, identities should be reauthenticated if the system detects suspicious behavior or before completing tasks and accessing data that are deemed high risk. The system may reauthenticate (or confirm) the user by having them sign in, providing a One-Time Password (OTP), or any other type of way to reconfirm it's the real user.
- **Authorization:** Authorize each identity with the proper permissions. What should this person/user/device/bot/

script/account legitimately have access to and what should they be allowed to do with that access? Just because a user has been authenticated doesn't mean that they should have access to everything within a system indefinitely. It's necessary to authorize the user to ensure that they're allowed access to the asset only when they need it and only with the level of permissions they need to do their job.

- **Access:** Provide access for that identity to authorized assets in a structured manner. How can the appropriate access be given to the person/user/device/bot/script/account and nothing more? By ensuring that only authenticated and authorized identities can access business assets, risks associated with identity-based attacks and identity hijacking can be mitigated. Additionally, businesses can structure accounts in a way that allows identities to be differentiated by whether an account is privileged or not. This segments high-risk activities into specific accounts that are used for a minimal amount of time to complete the required tasks while concentrating day-to-day work in identities with much more limited permissions. For example, separating regular user accounts for doing things like checking email from that same person's administrator account can help reduce the likelihood of an attacker getting access to the privileged identity and restricts the movement of the attacker within the identity with lower-level permissions. Similarly, not reusing non-human account credentials can provide a similar defense.
- **Audit:** Be audited or accounted for. How do you monitor the activities of identities? How do you reconstruct and analyze the actions an identity performed? How can all of this be verified to make sure it is happening the way you expected? Ideally, all systems would be perfectly secure and limit access to assets only after an identity had been properly authenticated and authorized; however, the reality is that human and technical gaps do occur, so it's important to have a system in place to audit the process to ensure that everything is correct and functioning as intended. A robust auditing capability ensures visibility into activities performed by an identity, provides context for the usage and behavior of an identity, and enables analytics that identify risk and provide insights to make smarter decisions about access. Taken together, auditing allows insight and evidence that Identity Security policies are working as intended.

REMEMBER

When you put all this together, you can form a quick story of how things should work in this model:

1. **A user logs into their employee desktop and is authenticated as an individual who should have access to the network.**
2. **They then navigate to the required assets (such as an application) and are authorized as someone who should have access to this application.**
3. **All access information is captured and analyzed for auditing purposes.**

Placing Identity Security at the Center of Security

After you understand the four As of Identity Security (see the preceding section), you must determine how to place Identity Security at the center of your information and cybersecurity programs, tactics, and designs within your organizations. If defending against bad things doesn't drive you to achieve this, then the balance of security and productivity should. Good Identity Security should achieve both.

Why traditional security is decreasingly effective

Securing computers, networks, and systems used to focus on the perimeter — the edge of the internal network that supposedly guarded you from what was on the other side of the wall. This way of thinking dominated IT-driven security strategies for decades.

Simpler times called for simpler solutions. But to keep evolving your thinking, take a look at these key points:

- **Security used to be simpler.** Your employees used to work primarily onsite or connected through a Virtual Private Network (VPN). They accessed your servers and applications, which were also onsite, from corporate-owned PCs. Fewer people needed access to critical business resources, and if

you had built a strong security perimeter, the bad guys were kept out, and your company was secure.

- **Digital transformation becomes a reality.** To gain competitive advantage (or because they didn't have a choice to *not* change), companies began rapidly adopting cloud-based technologies and services to deliver compelling digital experiences for their customers. Data workflows and applications, which were previously hosted on corporate networks, transitioned to public cloud infrastructure and SaaS. This transition accelerated during the COVID-19 pandemic shutdown, which forced businesses to embrace a work-from-home model. The digital transformation brought a shift from an enterprise-managed IT experience to a mix of personal and corporate applications accessed from personal and corporate-owned devices, where everyone wants everything to interact as seamlessly.
- **The perimeter security model is obsolete.** With digital innovation came new users and technologies (including laptops, mobile devices, and so on that never previously connected to corporate networks), putting increasing strain on the existing foundation of perimeter-based security approaches. These technologies also required new websites and apps to access network resources, as smaller screen sizes changed how much content could be displayed on the screen at a time. Remote workforces and numerous, varied types of devices needing to connect to critically sensitive company systems and data created thousands of entry points. Your network perimeter became even more porous and cyber attackers knew it.

This trend had been building up slowly for years, and the COVID-19 pandemic brought it into the spotlight, with an unprecedented sense of urgency.

New trends redefining approach to security

Recent trends, such as the adoption of SaaS and public cloud-based tools and work-from-home policies implemented because of the COVID-19 pandemic, have dramatically increased the quantities and types of identities in use within your organizations. Many companies shifted to the cloud (software, platforms, and

infrastructure) in broad efforts to reduce capital expenditures, embrace agility, and improve their technical capabilities. This pandemic forced a rapid overnight transformation, pushing many organizations toward remote work from home where employees connected from their own devices instead of connecting to an organization's internal network from company-owned devices.

Concepts and equipment such as VPNs, which were designed to create a secure tunnel for an employee laptop into the corporate network, became strained because they weren't built to scale to the new normal imposed by the pandemic when all a company's workforce now had to work remotely.

Businesses without a strong digital business model didn't do well in 2020. While most of the companies that weren't already fully virtual struggled to catch up, attackers moved quickly to focus their devious trickery and attacks on all the rough edges companies created out of haste. The monumental SolarWinds breach in 2020 defined and represented a new wave of attack methods, and successful bad actors in 2020 and 2021 pivoted to

- Ransomware everywhere all the time

  The surge in cyberattacks targeting both the lightly protected home office as well as critical infrastructure created unprecedented ransomware events across the globe.
- Attacks targeting cloud resources that were configured with excessive privileges
- Utilizing embedded application secrets, such as passwords, keys, or confidential logics within code placed in public repositories such as GitHub


TECHNICAL STUFF

In fact, a recent study by the Identity Defined Security Alliance (IDSA) found that 79 percent of enterprises experienced an identity-related breach within the last two years.

These modern computing and cloud risks already existed before 2020, but because the whole world was forced to adopt new cloud services to support their remote workforce, they took on new importance and urgency. It is now more vital than ever to transform your thinking to Identity Security, have an *assumed breach mentality* (which means that you design your security assuming the bad actor is already in your environment), and find ways to leverage more of Zero Trust.

Every identity can become privileged under the right circumstances

Although perimeter security is now effectively dead, the need to secure privileged access still remains. Both human and non-human identities can all become privileged under certain conditions. IT admins, remote worker, third-party vendor, device, or application accounts can all be compromised and elevated.

Working Better Together: Identity Security and Cybersecurity

In what has become an essentially perimeter-less world, it's virtually impossible for any organization to appropriately protect their most critical data and assets by focusing on traditional network perimeter-based security. In this new world, identity is indeed the new perimeter, and a Zero Trust approach based on Identity Security is essential.

Many companies still have Identity and Access Management (IAM) teams and program roadmaps that are separate from information security teams and program roadmaps. Identity Security goals and activities sometimes get spread across IT infrastructure, architecture, and security teams.

TECHNICAL STUFF

The *2021 Trends in Securing Digital Identities* report, by the IDSA, shows that the traditional organizational structure and approach is changing with IAM becoming critical to security strategies. In fact, 80 percent of the participants agree with the statement "Identity management used to just be about access; now it's mostly about security." Sixty-four percent report that they've made changes to better align security and identity functions within the last two years.

REMEMBER

Regardless of the reporting structure, Identity Security concepts, technologies, and transformation efforts need to be intertwined and aligned to the shift toward Zero Trust. IT and information security employees and leaders all face the challenges of enabling and securing applications, machine-to-machine access, and securing access and entitlements associated with the most sensitive and critical assets.

These critical areas share the common thread of Identity Security. More specifically as you look at IT operations initiatives led by your chief information officer (CIO), application development projects driven by the line of business, and the security professionals reporting into the chief information security officer (CISO), they all encourage reliance on identity as the foundational element of enterprise efficiency, effectiveness, and security.

IN THIS CHAPTER

- Pressing the gas on digital transformation
- Committing to the cloud and adopting more SaaS
- Making the move to work-from-anywhere
- Putting Zero Trust to work
- Seeing all enterprises as software companies
- Protecting your company from an evolving threat landscape
- Combatting increasing new threats to infrastructure

Chapter 2
Examining the Drivers for Identity Security

Identity Security, which is a foundational element of a Zero Trust approach, can help companies play offense by securing all identities, both human and machine, throughout the cycle of accessing critical assets to your company. This chapter dives into the key factors that make Identity Security the critical foundation for a modern cybersecurity program. You explore each one from a perspective that could form or influence a business case and help key stakeholders understand why this is so important. You also find out the various drivers for Identity Security and why it needs to be the "central nervous system" of your information security program.

Accelerating Digital Transformation

The criticality of Identity Security stems from the rapid acceleration of digital transformation across all industries. How companies do business is changing. Enterprise IT is changing. How (and where) the workforce operates is changing.

Companies embrace cloud-based technologies and services to provide compelling digital experiences for customers and to their increasingly distributed workforce. To truly benefit from this investment in digital transformation, they must fundamentally change how they do business internally, across distributed locations, and externally, with partners, suppliers, and customers. For all this to work seamlessly, Identity Security plays a holistic role.

TIP

These changes impact business operations, productivity, and profitability and come with the following benefits:

- **Speed and agility:** The agile business can quickly pivot to meet the needs of the customers, partners, and employees because new applications and application updates can be developed more quickly using cloud services.
- **Innovation:** Enterprises are improving customer experiences and leveraging technology to create new digital business models.

  Some examples of technology innovations that emerged as companies have digitally transformed their operations include

  - Widespread use of embedded financial technology, like digital wallets
  - Rapid adoption of telehealth, which bridged the communication between doctors and patients using videoconferencing over the phone or computer

    Telehealth was just getting started but rapidly accelerated during the COVID-19 pandemic.

Identity Security plays an important role in both examples because of the criticality of protecting these sensitive digital exchanges and interactions.

REMEMBER

While digital transformation gives businesses the tools they need to thrive in the marketplace, it also exposes significant risks because more data flows are exposed to external networks, applications, and devices. The days of unplugging a server to prevent access to data are gone and are replaced by digital tools that secure access. Think about your full ecosystem of access to your digital assets and all the people, companies, and information that you now need to protect.

Embracing Cloud Migration and SaaS Adoption

The digital transformation that businesses are undertaking has led organizations toward moving all or part of their on-premises data centers to the cloud, creating a need to secure data locally as well as in the cloud. Traditional cybersecurity measures that worked in the on-premises model are insufficient to reduce risk and protect important company assets in this hybrid environment, creating a need for new methods to secure information, data flows, and points of access. Further, the shared responsibility model (client and provider) for securing cloud services add further complexity, requiring enterprises to support and defend multiple different services with inconsistent control options across their public cloud and Software as a Service (SaaS) providers.

TIP

Although challenges exist, cloud-based services offer businesses multiple advantages:

- Efficiency increases from shared infrastructure costs, and you only pay for what services are needed at the time of consumption.
- Rapid provisioning and deprovisioning leads to increased agility, adjusting capacity and capability to meet business needs.
- Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and SaaS delivery complements DevOps processes.
- New capabilities, such as cloud-based Artificial Intelligence (AI) and Machine Learning (ML) services, enable new revenue streams and digital business models.

REMEMBER

While this change allows companies to create tools that drive business productivity and growth, it changes the magnitude of the threat landscape. Cybersecurity risks not only apply to data centers, but also security solutions must secure the development pipelines as well as their build and run-time environments while allowing frictionless access to the data and tools necessary for developers to make products that drive business growth.

Despite all the benefits of Cloud, the security challenges can often become overwhelming. If protecting the traditional data center is like protecting your house, spouse, and kids in a single-family home, the cloud security challenge is more like protecting your extended family, who are all living around the world in a combination of houses, campers, apartments, and lake houses. Identity Security is a way to make it all less daunting.

Shifting to Work-from-Anywhere

The COVID-19 pandemic accelerated an already existing, but slower moving, trend related to digital transformation — employees could now work-from-anywhere. Companies didn't have an alternative because most of their buildings were closed for an indefinite amount of time. Cloud-based solutions allowed organizations to continue developing and delivering products and services, even services such as healthcare.

The move to a distributed workforce wasn't without challenges because it required issuing new equipment or enabling employees to use their own personal devices to do work, deploying new and expanded collaboration tools, and expanding remote access requirements. The rapid growth of remote connectivity, unmanaged devices, distributed communication, and data transfers outside of enterprise networks resulted in a sudden and dramatic increase in the cyberattack surface and a related need for new cybersecurity approaches.

Acknowledging the Rise of Zero Trust

As businesses search for new ways to secure data, many have settled on Zero Trust as a preferred security approach. Zero Trust isn't a new cybersecurity model; rather it's replacing the old network-based model. The identity-centric focus of Zero Trust uses a holistic, strategic approach to security to ensure that every person and every device granted access are who and what they say they are. It achieves this authentication by focusing on the following key components:

- The network is always assumed to be hostile.
- External and internal threats always exist on the network.
- Network locality isn't sufficient for deciding trust in a network.
- Every device, user, and network flow are authenticated and authorized.
- Security policies must be dynamic and calculated from as many sources of data as possible.

By using these guidelines, a Zero Trust approach to security imposes access control across all networks, devices, users, and applications, by requiring continual verification of all human and machine identities. The focus is on the identity connecting to an application or infrastructure to secure the network instead of trying to fully lock down the boundaries of the network.

REMEMBER

The complexity of achieving Zero Trust has many nuances and can seem overwhelming. However, modern technology in Identity Security has made huge leaps to simplify user experience and efficiency while remaining effective. What once seemed appealing but impractical is much more of a reality.

Understanding that Every Enterprise Is a Software Company

Many industries have been radically transformed by software and digital technology. Photography and film was one of the first. Bookstores came next. Companies are not only figuring out

how to leverage software to better run their operations, but also they're using software to transform how their businesses interface with customers. An industry's product itself may be shifting from physical to digital. To do this, companies must control the design, execution, and operations of their entire customer experience. This process may also include having to reimagine the product itself.

As software becomes the pulsing heartbeat of many companies and industries, this new normal has resulted in an explosion in the number of internal and external identities that an organization must manage. This expansion of identities has also increased the number of access points for malicious actors, which makes the need to secure identities even more critical.

REMEMBER

The shift to software and digital-led business model means that the effort to secure the expanding landscape of identities is increasingly critical. Ensuring your Identity Security focus is keeping pace with, or even ahead of, your digital transformation can help make security an enabler rather than an impediment.

Defending Against an Evolving Threat Landscape

As businesses increase their productivity and efficiency, additional risks may occur. Attackers never stop innovating and are taking advantage of new technologies and platforms to create new technological threats. Ultimately, almost every new approach that these bad actors can dream up ties back to some form of trickery that compromises an identity or account. From there, they always find ways to pivot higher stakes identities and more appealing company "crown jewels" (what you value most).

WARNING

If a business or technology leader ever tells you there is no need to worry about information security because your company leverages world-class cloud providers, don't fall into this trap. Spend the time educating them on all the work required to secure cloud or multi-cloud environments for your company that large cloud providers don't and can't own. You can't outsource accountability or business risk.

Ransomware isn't new, but it has continued to increase in popularity and consequence over the past few years. As ransomware attacks increase in prevalence, the tactics employed by malicious actors have morphed, increasing pressure on organizations to pay the ransom.

Malicious actors operate as businesses, selling hacking services that enable cyberattacks to actors that would otherwise lack the technical expertise to launch the attack themselves. Additionally, these "anti-security" services are often mature, meaning that they already have the infrastructure necessary to carry out coordinated cyberattacks at scale. Moreover, payment for these services are made in cryptocurrency, which allows for quick, inexpensive payments with increased anonymity for cybercriminals.

Increasing Threats to Supply Chains and Critical Infrastructure

As supply chains and critical infrastructure adopt cloud services to benefit from increased efficiency, scalability, and costs, it exposes them to additional cybersecurity threats. Bad actors are increasingly drawn to these high-value targets, which are associated with massive ransom demands. Identity Security plays a foundational role to defending against both supply chain and critical infrastructure focused attacks.

Attacking supply chains

Supply chains are an attractive target for attackers due to the extent of their reach into corporations and governments around the world. These organizations are well funded and require supply chain inputs to function. Disrupting the supply chains applies extreme pressure on organizations to pay large sums of money to re-establish their functionality, making them an especially high-value target.

Securing the supply chain has become an increasingly difficult task. As supply chains evolve to become more intelligent, efficient, and automated, they now expose themselves to increased numbers of human (third-party vendors, remote workers) and machine (applications, Internet of Things [IoT] devices)

identities, each of which requires access to supply chain data. This extended supply chain is a conduit for cyberattacks and thought to be responsible for 40 percent of attacks on companies, according to a report from Accenture. By focusing on Identity Security, supply chains can be managed in a way that grants appropriate permissions to identities while protecting the underlying assets from attack.

Threatening critical infrastructure

While the rise of ransomware has led to a spike in financially motivated cyberattacks, activity driven by nation states and state sponsored threat actors has also increased dramatically in the past several years. These threat actors often work on a longer timeline due to strong financial backing, patience, and persistence, and they employ a level of sophistication that's far greater than other bad actors. In many cases, these attacks play out over many months or years, and the focus on critical infrastructure means that the consequences can be far reaching.

In attacks against critical infrastructure, threat actors are looking to disrupt control systems rather than extract data to exploit the systems for ransom. These attacks can target the utility grid, public transportation, public services, and telecommunications systems, and breaches can result in catastrophic outcomes. Many critical infrastructure sectors rely on older technology to function. This prevents a challenge for securing systems because some of this technology has many years' worth of vulnerabilities that attackers can exploit. Given the importance of these sectors to everyday life and national security, secure these systems against attack is critical.

IN THIS CHAPTER

- Outlining digital identities
- Getting to know the Identity Security model
- Assembling essential Identity Security controls

Chapter 3
Understanding the Controls Needed for Identity Security

Unfortunately, in some organizations, security projects consist of buying a new tool, assigning engineers, and turning it on in hopes that the organization is now "more secure." That approach falls short of expectations, and organizations fail to capture the potential value of their investment. The same is true in Identity Security initiatives: The hardest parts are creating understanding, securing organizational buy-in, managing the organization through the change, and scaling your solution(s) to the areas of your business that need it most. You need to master the key controls that make up Identity Security to lead your organization through the changes that are necessary to achieve a successful implementation, and ultimately, meet your business goals. Understanding and helping key stakeholders and users of an Identity Security program comprehend what elements of change will be required is the first step.

This chapter unpacks the key controls that make up the foundation of an Identity Security initiative that secures all identities, whether human or machine, and dramatically improves your organization's security posture.

Defining Digital Identities

A *digital identity* is a collection of metadata (descriptive information) that uniquely defines an entity (something or someone). System entities interact with resources, such as a computer's central processing unit (CPU), and objects, such as files, to complete work. In more familiar terms, an identity is an account or a persona that can interact with a system or application.

REMEMBER

With different roles and levels of access to information or services, many different types of identities exist:

- **Human identities:** Humans interact with computers and applications. Examples include
  - **System users —** employees, contractors, customers — with basic-level access to use the system as intended
  - **Elevated users** — helpdesk staff, SaaS administrators, managers — who can make significant changes within a defined set of functions and see more data
  - **Administrative users** — domain, cloud-tenant, or database administrators — with complete authority to make changes within their scope
- **Non-human identities:** Automated or backend functions should proceed without human involvement. Examples include
  - **Devices:** Real-world physical objects like cameras, locks, sensors, and so on

    Increasingly, these devices also have identities that need to be managed as more devices are now part of the Internet of Things (IoT).
  - **Service accounts:** Allow applications and service access to other resources like databases, other systems, and web services

- **Robot accounts:** Allow an autonomous application that usually acts on behalf of a user to take some actions independently using its own access mechanism such as a chat bot, Artificial Intelligence (AI) algorithm, or workflow engine

Understanding the Identity Security Model

Identity Security brings a security lens to traditional Identity and Access Management (IAM), which has historically focused on ensuring that tactical access needs are met as a priority. By combining IAM and key security functions, the Identity Security approach gives enterprises a powerful new set of tools to protect their assets.

In the Identity Security model, IAM is combined with Multifactor Authentication (MFA), Privileged Access Management (PAM), and Identity Governance and Administration (IGA) tools to substantially transform and harden the identity perimeter. A comprehensive Identity Security architecture then moves the organization toward seamless integration of Identity Security with Security Information and Event Management (SIEM), Security Orchestration Automation and Response (SOAR) platforms, Data Loss Prevention (DLP) tools, Endpoint Detection and Response (EDR), and the rest of the security operations stack to provide powerful security operations capabilities. For more information on the security stack, see the later section "Infuse identity into your security operations."

Building Your Essential Identity Security Controls

Embarking on an Identity Security initiative transforms your organization in many ways and is a foundational step to moving to a Zero Trust model. The Identity Security controls implement the four As by focusing on securing individual identities throughout

the cycle of accessing critical assets. Check out Chapter 1 for more information on the four As of Identity Security.

In order to successfully implement the Identity Security model, essential controls must be addressed. Each control plays an important part and can be implemented in a few ways, allowing organizations to prioritize based on risk, existing investments, and organizational appetite for change. I cover these controls in this section.

REMEMBER

These essential controls combine to create the foundation of a robust Identity Security approach and offer organizations several choices in how to implement them that can be aligned to overall business and security objectives. By taking a holistic, thoughtful approach to Identity Security controls, organizations can help users get to the applications, infrastructure, and data they need in a secure way and lay a strong baseline for Zero Trust as well.

Centralize identity and access

Centralizing identity and access with SSO and directory services is a priority for successful Identity Security initiatives. Identity Security architecture leverages Access Management (AM) to empower workers and customers with easy, secure access to the apps and resources they need, from any device, location, or time. Users should experience seamless access across devices and services, with AI ensuring threats are kept out. Many organizations have built manual access management processes that have become siloed and fragmented across the organization. Standardizing and automating these processes is key to truly attaining the value of an Identity Security program.

Business networks are complex, especially at scale, so enterprises use directory services to map the network. These services store information about the business infrastructure, including folders, files, printers, employee information, passwords, and much more, and can be hosted onsite and in the cloud. Directory services also map the relationships that users have with the data, which means access can be limited to resources that are appropriate for their job responsibilities. Unfortunately, as networks expand, the directories can become scattered across different services, which increases cyber risks because IT professionals must coordinate access control between multiple platforms.

A key enabler of an Identity Security architecture is the centralization of directory services to control access across multiple platforms, which also results in a more efficient and robust security infrastructure. This should include on-premises and cloud directories, such as Active Directory (AD), Azure AD, and Lightweight Directory Access Protocol (LDAP) directories. Additional directory types, such as HR systems, should also be included in this consolidation. For identities that aren't currently centralized, directory services can securely store users, groups, attributes, policies, and credentials within an extensible directory service.

Single Sign-On (SSO) is an equally powerful tool for enabling user experience and enhanced security. By linking applications to central identity and access services (using federated approaches such as Security Assertion Markup Language [SAML], Open Authorization [OAuth], Open ID Connect [OIDC], and other techniques) end-users are presented with seamless, low-friction experiences as they navigate through applications and data stores throughout their activities. By reducing the number of passwords and authenticators that the user needs to manage, the overall attack surface becomes a positive user experience.

Deploy risk-based MFA

By centralizing core IAM functions with SSO and Directory Services, the Identity Security model streamlines the deployment and use of essential related technologies like adaptive MFA. Because an SSO-enabled identity has tremendous access and privilege within the organization, layering on additional protections is crucial.

MFA is a great tool for authenticating and securing account access; however, constant or repeated MFA challenges (prompting a user to authenticate) can be burdensome to users by interrupting workflow. A well-architected Identity Security process and platform uses intelligent monitoring to challenge users with MFA based on dynamic conditions, like location, device, day of week, time of day, and even risky behavior. Additional controls allow MFA challenges to monitor even more granular data, including device ownership, management, location, and security posture. Intelligent automation of MFA challenges allows IT professionals the ability to build a network that's effectively able to secure important assets while causing minimum impact on user efficiency — a key to scaling Identity Security across all users in an organization.

Secure privileged access and manage entitlements

After IAM functions start to become centralized, the next order of business should be to tackle privilege in the environment. Protecting privileged access reduces the impact of an attack and protects access to critical resources. For this reason, many enterprises employ a least privilege approach, where access is restricted to the resources necessary for the end-user to complete their job responsibilities with no extra permissions. This approach is often done using just-in-time (JIT) techniques that dynamically elevate privileges only when needed.

Privileged accounts are accessible by those users and services that require elevated access to systems, and these accounts can make changes that affect the structure, functionality, and integrity of the system or network. These accounts are often shared by multiple users.

REMEMBER

To achieve Identity Security, these privileged accounts should be managed and secured with a technical solution that can automatically rotate the password periodically and after each use. Because the password is rotated, even if it's copied down, it can't be reused. As a bonus, by letting a tool manage the password, the password can be more complex because there's no need to copy it down on notes or spreadsheets (or worse, putting it on a whiteboard in someone's office).

Along with rotating the credentials of privileged accounts, access should be recorded and centrally stored to make it easy for security, audit, and compliance teams to increase accountability and compliance. Session recordings can be used to efficiently and completely reconstruct any privileged access use in an organization and tailored based on risk tolerance so that only the sessions needed are captured.

In addition to privileged access, entitlements and permissions that allow privileged actions should be carefully managed. Cloud Infrastructure Entitlement Management (CIEM) solutions can add important and flexible capabilities to an Identity Security architecture, based on organizational needs.

Automate governance and the identity life cycle

Invest in automating the life cycle of identities. In fact, much of the effort in other controls lends itself to supporting this automation that in turn enables organizations to efficiently govern their entire set of identities.

The traditional AM process is laborious and complex: requesting, approving, provisioning (granting), deprovisioning (un-granting), controlling privileged access, and doing all the preceding for vast numbers of identities and accounts. The added effort required to conduct periodic reviews across IT assets (systems, databases, hardware, cloud) is significant. For many companies, these tasks represent multiple full-time jobs.

Automated provisioning and life cycle management in the Identity Security model enables dynamic provisioning and de-provisioning of access that can become especially important when employees leave an organization. It also lets users and administrators request access and define custom approval workflows that meet the need for the organization.

Periodic access reviews are one of the key controls for many organizations. These reviews are often slow, manual, and error prone. A more modern approach to Identity Security will include automating many components and streamlining review processes. This is especially important as access decisions and privileged roles spread out to business roles (for example, an HR manager) because it may be tough for an IT administrator to know who should have access to what. The Identity Security model enables the access review process to be executed by those who know who should have access regardless of their role in the organization.

Integrate identity with endpoint security

In many enterprises, users are given local administrator access to their computers to reduce the burden on helpdesks for installing software or correcting issues. Unfortunately, this access also means that malicious software can gain a foothold by using users' access, potentially compromising not just the endpoint but any other systems that the users can access. This is a common attack path when it comes to ransomware, and as a result, protecting

endpoints has become a vital part of a robust Identity Security program as well as a core tenant ensuring Zero Trust.


TIP

To achieve Identity Security, leverage Endpoint Privilege Management (EPM) tools, locking down local admin permissions to the minimum necessary for users to do their daily work and providing a mechanism for controlled escalation, either of their own account or a managed administrator account, when necessary. These limitations include what software can be used, installed, and executed on the endpoint and stops the abuse of local credentials on desktops and servers, helps contain the spread of malware, and prevents attackers moving laterally in the enterprise.

In addition to reducing persistent privilege on the endpoint, the endpoints themselves should also be authenticated under the Identity Security model. You can accomplish this feat with a variety of technical and procedural controls but it's most frequently done with certificates that are provisioned onto the endpoints. Checking for these certificates can give further assurances about the user and device.

Infuse identity into your security operations

Integrating your Identity Security with your security operations ecosystem enables powerful protective and detective information security capabilities. Organizations will gain significant preventative security capabilities from the investments that are essential for Identity Security implementations. At the same time, the effort to implement Identity Security controls will also increase visibility, decrease investigation and response time, and ultimately make the security team more capable and efficient.

Complementary controls can help improve security operations in the following ways:

- **User and Entity Behavioral Analytics (UEBA)** tools bring deep insights about normal and irregular behaviors within the ecosystem. By centralizing IAM as part of an Identity Security architecture, the UEBA tool deployment is simplified and can start to show value immediately.
- **Security Information and Event Managers (SIEM)** benefit from access to a single source of truth about identities and

access privileges in addition to simplified integrations with fewer log sources. This is an advantage because alerts can surface more quickly, and analysts have immediate access to vital contextual information during investigations.

- **Security Orchestration and Automated Response (SOAR)** tools also gain new powers. Using the integration and automation already present in Identity Security control implementations, the SOAR platform enables security analysts to react in near-real-time to prevent and disrupt active attacks by blocking access, forcing reauthentication, or rapidly removing compromised users.
- **Cloud Access Security Brokers (CASBs)** use seamless integration between different identity and authentication services to ensure that security controls for cloud services are enforced across all users and devices. CASBs also provide security teams with information about Shadow IT in the enterprise and help identify new applications that need to be secured with the appropriate Identity Security controls.

IN THIS CHAPTER

- Keeping in mind never trust, always verify
- Understanding Zero Trust
- Getting to Zero Trust with Identity Security

Chapter 4
Achieving Zero Trust with Identity Security

Traditional perimeter-based security strategies treated networks like a classical Greek City-State. If the walls remained strong, they provided a good defense for the city and repelled invaders, keeping the citizens of the city safe. But even in Greece, the Trojan Horse was used to sneak soldiers into the fortified walls, leading to the fall of the city of Troy. There were too few defenses inside the walls of the city to keep it secure once the walls were breached. Similarly, perimeter-based network security strategies also fail once attackers breach the defenses; the old way of thinking will no longer cut it. The perimeter-focus is dead.

Modern attack methods coupled with shifts from traditional data centers to the cloud means you must shift your thinking from a focus on securing the perimeter to a Zero Trust minded strategy. Your networks must not fail in the same way that a perimeter defense focus failed Troy. Even though you allow users access to on-premises and cloud-based applications and resources (like the Trojan Horse entering through the walls of Troy), it doesn't mean that they have freedom to move around carte blanche; users must be monitored and permissions removed in case of suspicious behavior. Additionally, modern tools make it easier to achieve a Zero Trust strategy. In this chapter, I go more into depth into the concepts and how they apply to Identity Security.

Remembering "Never Trust, Always Verify"

In the traditional IT security models, you assume that systems and traffic within the confines of the corporate network can be trusted. But when using Zero Trust principles, you should assume that the bad actors (whether external attackers or malicious insiders) are already in your network and have access to your applications and systems.

REMEMBER

Simply stated, Zero Trust works on the principal of "never trust, always verify." This means devices and identities shouldn't be trusted by default, even if they're connected to a managed (and "secure") corporate network. They must be continuously verified.

The first evolution of Zero Trust attempted to push network perimeters closer to the resource needing protection (for example an app server) by requiring authentication and authorization for access inside these smaller, more specific network segments, which is termed *micro-segmentation.* Think of this like digging small moats around different parts of the city that you want to protect.

WARNING

The challenge of setting up micro-segmentation comes down to complexity. The most segmented setups stifle movement, while larger segments are more porous, resulting in greater losses in case of breach. Relationships between the segments are constantly shifting (a reality of networks), and an approach based on micro-segmentation alone is insufficient for securing networks.

The only real option left across all networks, devices, users, applications, and so one is to adopt a Zero Trust approach based on Identity Security centric controls. The bottom line is that with Zero Trust, no actor, whether human or machine, can be trusted unless they're continually verified based on risk. It's a holistic, strategic approach to security that ensures that everyone and every device granted access is who and what they say they are. "Never trust, always verify."

Defining Zero Trust

Throughout this book, I cover the basics of Zero Trust: conceptually, historically, and going forward in your modern world. In this section, I define Zero Trust from an Identity Security standpoint in context of how it is done.

Verify every user

Making sure people are who they say they are may sound obvious, but it often goes wrong when organizations rely on only one verification method like a single set of credentials that are easily stolen or compromised. In these instances, the continual verification element of Zero Trust comes into play. Additional verification may be required, depending on the level of risk of the action.

Even with systems performing additional verification mid-session, the security is still not strong enough if it relies on a single factor (password) for reauthentication. This is especially dangerous when used in combination with Single Sign-On (SSO), which is a technology to use a single login and "pass-through (modifies access)" to other applications once you're logged in. This can allow broad access to many systems and applications (which is great for productivity and bad for attaining Zero Trust if not combined with additional Identity Security controls).

To avoid this problem, SSO needs to be balanced with other technology such as Adaptive Multifactor Authentication (MFA). Adaptive MFA technology uses intelligence to determine whether additional verification should be required, based on many different risk factors. For instance, additional verification may be required after there are several unsuccessful login attempts, when a new IP address is used, or if a privileged account is being accessed. New technologies can move authentication to a password-free experience by using biometrics, security keys, and specialized mobile applications. These technologies combined with SSO create a tight web of security around an organization's network.

Validate every device

While user verification adds a level of security, it's not enough to secure networks from attack. The Zero Trust model requires that all devices be authenticated and associated with verified users

before allowing access to resources. This requirement greatly limits the number of access points that an attacker can use to access the network.

After a device has been validated and verified as belonging to an authorized user, risk-based access intelligence can be further used to reduce the attack surface. This allows aspects of the security posture of endpoints, like device location, a device certificate (an identifier unique to a specific device), OS, browser, and time to be used for further access validation.

While device validation is a great tool for limiting the attack surface, remember that device validation is only as reliable as the security of the endpoint itself. While most businesses recognize the importance of running antivirus software to secure endpoint devices, additional tools can tighten security even further:

- **Application patching:** Applications contain bugs and security vulnerabilities that developers frequently fix via security updates. To stop attackers from exploiting these vulnerabilities, keep applications up to date.
- **Operating System (OS) patching:** An OS requires patching in a similar manner to applications. These patches include both non-security critical patches as well as security patches, which fix known vulnerabilities. Patching the OS ensures that all known issues have been addressed.
- **Privileged Access Management (PAM):** Applying least privilege limits access rights for users and running processes by only assigning the least amount of access privileges required to complete the job. This includes removing local admin access from endpoints, which substantially improves security by removing a common access point for attackers.
- **Endpoint Detection and Response (EDR):** EDR is a technology that collects, records, and stores large amounts of data from endpoint activities. This provides visibility for detection, investigation, and mitigation of security threats.

Intelligently limit access — including privileged access

After you've verified the user and validated the device, you're all set, right? While these steps help secure the network, they are still insufficient. Under a Zero Trust model, you assume that bad actors have infiltrated the system, so you've got to limit damage if the verification and validation steps are inadequate. The best way to limit damage is to follow a principle of least privileged access where individual identities should only have access to what they need for only as long as they need it. This restriction helps limit the attack surface even further.

Limiting access can be done manually by assigning the appropriate account permissions for a job and removing them afterwards; however, this requires additional IT resources to accomplish, so the timeliness of revoking privileges is generally delayed (if it happens at all). Luckily, tools now exist that allow for automated Just-In-Time (JIT) access, which raises privileges for a temporary amount of time and then removes them afterwards. This automates the process of managing privileges and helps limit higher level privileged access even further.

For example, a standard user whose job it is to enter data into a database has specific privileges allowing them to only enter records. In case the account is compromised, these low-level privileges limit the attacker to only adding records to the database. While this might result in inaccuracies in the database, it is far less damaging than if the attacker had full access to delete or export data.

Identity and context-aware controls can be used to intelligently limit privileged access to cloud resources. For this to be effective, it is important for an organization to have a map of whom (human and non-human users) has access to which resources, when and what actions they are authorized to perform. By enforcing the principle of least privilege broadly in addition to verifying users and validating devices, organizations reduce the risk of malicious actors progressing their attacks and decrease their overall cyber security risk.

Achieving Zero Trust with Identity Security

Cyber threats are always evolving. The perimeter-based approach of security from the past is no longer effective in preventing breaches of hybrid environments. Zero Trust is the best model for securing applications, infrastructure, and data from unauthorized access, and Identity Security controls are foundational to make that happen.

For enterprises that are looking to implement Zero Trust using Identity Security, to start you on your journey, consider these key factors:

- **Mature existing Identity Security controls and evolve into advanced controls over time.** By examining existing Identity Security controls and policies, enterprises can identify areas that require additional security tools. Oftentimes, tools exist that just need to be enabled or their use expanded, and these tools can dramatically decrease the security risk. For instance, instead of allowing users to log in with just a username and password, MFA and SSO can be implemented, which decreases the friction for users while increasing the security for the enterprise. It's a win-win situation. For enterprises desiring stronger security controls, advanced Identity Security tools can help by constantly monitoring identity usage for suspicious activity, blocking suspicious activity, and requiring additional authentication.
- **Look for new opportunities to shore up Identity Security across the enterprise.** Using the principle of least privilege, enterprises can limit damage that malicious actors can cause by limiting permissions to identities based on what is needed. Some low-cost ways this can be achieved include removing local admin accounts, ensuring limited access, and providing privileged users with separate accounts for daily tasks and administrative tasks. For enterprises needing a stronger layer of security, JIT access to privileged accounts limits the time that higher risk compromises can occur.

IN THIS CHAPTER

- Breaking down the problem
- Knowing where to focus first
- Sharing information with your peers
- Choosing a vendor strategy

Chapter 5
Getting Started with Identity Security

My biggest tip and lesson learned from building and deploying technology, processes, and growing human capital around Identity Security is that planning and prioritization are critical. These tasks are so important in Identity Security because of the broad scale of identities, infrastructures, and applications that must be secured to achieve a Zero Trust, informed Identity Security capability. This chapter explores planning and prioritization and helps you learn how to get started with Identity Security and sets you up for success.

Breaking Down the Problem

Plans for anything in work or life are more attainable if they can be broken up into achievable milestones that align to the goals you want to achieve. To do this, focus on identifying the most important business assets that require protection and understanding the existing security risks that put those assets in jeopardy. This level of thinking is all about comparing risk reduction value to level of effort and starting on the most impactful items

first. Some actions and milestones to take within your planning phase include the following:

- **Identify risk.** Understand what security controls you have already applied to which assets and where the biggest risks exist. This allows you to make more informed decisions for how you want to focus your Identity Security efforts moving forward.
- **Prioritize use cases.** Take stock of your internal priorities. Are there audit and compliance requirements? Did you have a security incident or breach? What IT assets are most critical to the business? With this input, weigh each use case against the risk, impact, and effort. A phased approach connected to business outcomes gives you maximized momentum and business buy-in.
- **Align to business outcomes.** With risk identified and use cases prioritized, you can align your desired use cases to business outcomes. It is important for the effectiveness and buy-in of your program to emphasize how your Identity Security program will reduce risk, improve operational efficiencies, streamline audit and compliance efforts, and enable digital business initiatives.
- **Create your roadmap.** Begin to map your journey by focusing on risks that are most impactful to your business. You may not be able to do everything at once, so prioritization and focus is the key to a successful roadmap execution.
- **Get executive buy-in.** Getting executive sponsorship starts with showcasing how your program will meet your organization's risk reduction and compliance goals to support business initiatives.
- **Communicate your plan.** With a plan in hand, it's time to communicate it to others within the organization so that it becomes the company's plan. Be sure to work with your internal teams and executives to align your plan to the business goals and needs of the workforce.
- **Facilitate end-user adoption.** Identity Security is a team sport. To meet risk reduction, it's crucial for technology owners, developers, and end-users to embrace your Identity Security controls.

Seeing Where to Focus

After or during your identity/account inventory process, you need to determine a method to evaluate risk. You can't fix everything at once, and most organizations determine where to start by using a risk-based approach. First, make sure the basics like Multifactor Authentication (MFA) and Single Sign-On (SSO) are applied holistically across the organization. Not having them in place increases your risk and makes your company an easy target for an attacker foothold. From there, use risk-based prioritization by identifying the following:

- The organization's most critical systems (if you have a system classification process or a list of critical systems ranked by confidentiality, integrity, and availability concerns)
- Systems that contain data that needs to be secured due to regulatory requirements
- Systems with intellectual property or customer data
- Known vulnerable systems (if issues have already been identified from audits, pen tests, and so on)

Learning from Your Peers

The best thing about the cybersecurity field is the willingness and openness to share and learn from your peers, even with competitors. This isn't typical and is made possible by almost all companies fighting against the same threats.

If you don't have a robust external network of peers, invest time in forming these relationships. Options include the Information Sharing and Analysis Center (ISAC). These non-profit organizations provide a central resource on cyber threats to critical infrastructure and providing two-way sharing of information between the private and public sector. Additionally, other cybersecurity-related learning and sharing organizations are relevant to Identity Security. These include the Cloud Security Alliance, Cloud Native Computing Foundation, and the Identity Defined Security Alliance.

REMEMBER

Ultimately, the most important indicator of success of a sharing and benchmarking organization where you might spend your time is how active the community is. You get out of it what you and your peers put into it.

Opting for a Single-Vendor versus Multi-Vendor Strategy

When it comes to selecting technical solutions, enterprises tend to fall into two camps: One tends to buy best-of-breed solutions and spend resources on integration efforts, and the other tends to select integrated platform capabilities and spend resources tailoring and customizing for special cases. However, when it comes to Identity Security, all enterprises should consider an integrated platform rather than build their own solution using a collection of products.

TIP

With an integrated platform, Identity Security becomes easier to implement and provides a powerful foundation for the rest of your enterprise. Other reasons to choose an integrated platform include

- Reducing complexity and risk with greater interoperability across security tools
- Enhancing visibility with a unified view of risky activities for identities of all types
- Improving operational efficiencies with one administrative console across multiple Identity Security controls
- Realizing cost savings through vendor consolidation

For more information on how these key controls intersect with Identity Security platform approaches, see Chapter 3.

A build-your-own approach may make sense, though, in a couple of cases:

- You have significant existing investments in multiple existing Identity Security capabilities from different providers.
- You have complex custom workflows implemented in a tool that doesn't offer all needed capabilities.

IN THIS CHAPTER

- Prioritizing your Identity Security landscape
- Discovering new targets for attacks
- Ensuring effective MFA implementation
- Using PAM for high-risk access
- Enabling JIT access
- Driving cultural change

Chapter 6
Six Actions for Success in Identity Security

A majority of breaches tied to hacking involve lost or stolen credentials or using brute force to obtain credentials. This may not be surprising because identities exist across organizations at every level. It may be easy to get overwhelmed with the span and scope of the challenge in front of you, though. But whether you're just starting your Identity Security program or taking it to the next level, check out this chapter. I give you six action items for driving focus, execution, and overall success within your organization.

Identify and Prioritize Your Identity Security Landscape

Many organizations struggle with (or even neglect) comprehensive IT asset inventories (devices, accounts, data, services, and so on) and don't manage the life cycle of their IT assets from onboarding to end of life. It is hard to protect what you don't know about. This gap situation can lead to overlooked service accounts, workers using unmanaged devices, poorly controlled

third-party user access, improperly de-provisioned user access following separation from the company, and more. These challenges need to be rapidly addressed, but you can't do everything at once.

TIP

First, identify the systems and data that are most likely to be targeted by an attacker, and then identify which people and machines can access them. Attackers will target IT assets either because they may hold your most valuable "crown jewels" (sensitive information) or because they may want to use that IT asset as a foothold to pivot to something even better.

REMEMBER

As you inventory and prioritize the focus of things to adapt into your Identity Security program, keep these two questions in mind:

- **Where are my crown jewels?** Classify what's most sensitive to your business. Decide what information or systems would knock your company out of commission or place it in a compromised situation if your valuable assets were stolen or manipulated.
- **Where can bad actors enter or exploit my organization?** Intersect crown jewel assets with vulnerability scans and penetration test findings to prioritize the most vulnerable high-risk assets.

Prioritize starting with the systems that meet these risk-based criteria first. You can't do everything at once, so why wouldn't you want to start with what's most important?

Discover "New" Targets Subject to Increasing Attacks

Your system admins may think they know who or what's authenticating to their applications, databases, or services, but you should always follow the data to see what new targets or exploits are emerging. You can find high-risk service, DevOps, cloud service accounts, and more in these common ways:

- Use analytics and automation to sift through logs for sensitive databases and applications to find where logins are coming from.

- Connect to procurement processes so potential account sources can be flagged as they come into the organization.
- Use manual account management processes to uncover new sources of accounts through organic means as users start to share new capabilities and their presence in the organization grows.

You can also use similar processes to find *new* types of privileged accounts that need to be protected. These accounts include admin and developer accounts for Multifactor Authentication (MFA), Single Sign-On (SSO), and Public Key Infrastructure (PKI) as well as service accounts for analytics and Artificial Intelligence (AI).

Innovative programs and tactics driven from digital transformation efforts require you to look in novel places for the identities you must protect, especially as privilege moves away from traditional IT administrators to business and front-line users.

Ensure Your MFA Implementation Is Effective

MFA has grown to be one of the most important controls to prevent a stolen credential from becoming a hacked account. However, it's *not* perfect. Red teams and real attackers have proven that they can trick users into giving up their second (or third) factor. Help desk workers can be socially engineered into resetting MFA accounts for an attacker.

TECHNICAL STUFF

A *red team* is a group that plays the role of an enemy. They're authorized to operate in this manner to help find exploitable gaps. They can also be referred to as *threat hunters* or *penetration testers.*

TIP

To thwart the bad actors from circumventing your important controls, take the following practical actions:

- Reduce manual password usage by using standards-based SSO and methods such as device certificates (embedded digital identifiers within company approved devices), biometrics (facial images, fingerprints, and so on), and push notifications (pushing a verifying action to a smart device).

- Lockdown MFA registration by using an out-of-band process to verify a request made by a legitimate user. This means that the agent resetting MFA should take some action such as calling the requestor back at a company directory authorized number.
- Have the security team own the user experience for authentication and make it frictionless for the user. Design the flow to present reauthentication requests sparingly and when a user may expect them, such as when using a powerful function or doing something outside of the norm. The security team must accept accountability for ensuring that the bad actors are stopped while the user experience isn't forgotten.

Protect High-Risk Access with PAM

Privileged Access Management (PAM) solutions have historically been used to protect administrative access to infrastructure and sensitive applications. While this is imperative, Identity Security can only be fully realized if it reaches beyond back-office IT administration to other users — such as line of business users and developers as well as machine identities and their associated secrets — with high-level and high-value access. Ensure secure access at scale to wherever sensitive data flows and is used without burdening humans or machines.

Securing privileged access is central to reducing the impacts of attacks and protecting access to critical resources. Also, in a newly hybrid, dynamic world, it's especially important to use a least privilege, Just-In-Time (JIT) approach to give elevated access for only a specific amount of time to resources necessary for users to do their jobs.


TIP

Applications are the place where information, data, and context are all brought together for use. At a minimum, use PAM technology for all application administrator accounts, emergency "break-glass" accounts (used as a last resort in emergency situations), and any end-user accounts that are shared by multiple users.

TIP

Consider using a PAM system to implement dual control and/or session monitoring for sensitive functions, for higher-risk service accounts, and for personal accounts (such as executives) when accessing extremely sensitive information.

Allow Just Enough Access

Just enough and JIT are important concepts to reach Zero Trust principled Identity Security. Consider this analogy: Say you have a collection of historic gold coins that you keep in a lock box at a bank. Do you have a lock box key for other bank patrons? No, you just have yours. Can you access the bank anytime without any help or anyone else there? No. Most bank lock box processes enable access when you need it with a key, plus a bank official signing you in and out and monitoring other events that may be suspicious. Managing privileged access in a JIT fashion and with just enough permissions works in a similar way.

REMEMBER

You can accomplish these techniques with a combination of technology and processes. However, choosing the right technology is key because most human-managed processes can't enable a true JIT outcome. To make this concept more actionable, consider the following key takeaways:

- Limit user connections to a single resource or narrow subset. Options include proxy technologies and Virtual Desktop Infrastructure (VDI). Use tiered jump servers (bastion hosts) to connect admins to infrastructure. Isolate unmanaged devices connecting to corporate resources to reduce the risk of malware spreading.
- Minimize local admin access. Consider using endpoint protection technology to restrict installations to whitelisted or greylisted applications.
- Provide JIT access at the right time and place for a limited period from your PAM system.
- Make JIT easier to use and audit via automated approvals, adjusting the period that the access is open for when needed and using a ticketing system for access requests. Combine this with continuous session monitoring and recording for an audit trial of actions taken during the JIT session.

Drive Cultural Change within Your Organization

Identity Security with Zero Trust isn't just a set of controls; it's also a mindset and requires a cultural shift that demands involvement and action from stakeholders beyond traditional IT infrastructure and security teams.

To be successful, the chief information security officer (CISO) and key Identity Security team members need the support and engagement of stakeholders who influence change throughout the organization. Modern cybersecurity programs require a lot more sponsorship outside of IT than they did decades ago.

Identity Security should be viewed as a journey, not a sprint. While quick action and risk reduction can be attained, deploying Identity Security controls across mid- to large-sized organizations will happen in iterations with increased depth and effectiveness. Use Key Performance Indicators (KPIs) to track performance over time.

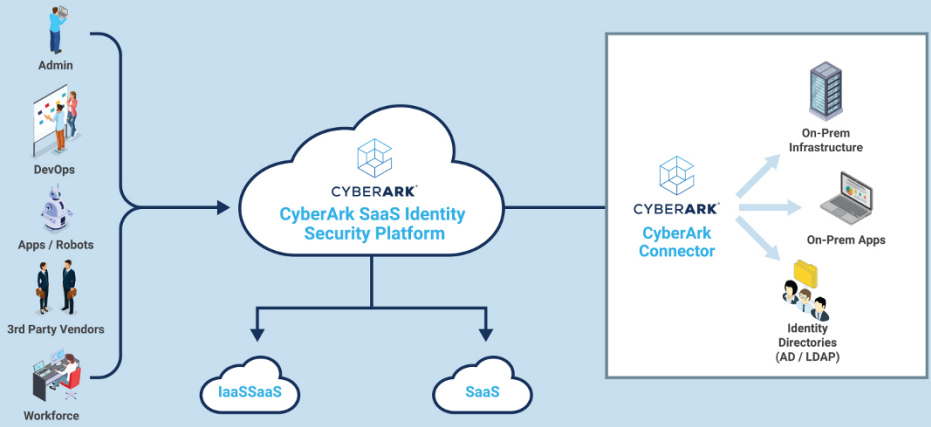
TIP

Communication and Organizational Change Management (OCM) is critical to a successful program. Program leaders should convey the following key messages within the company:

- Share that having less privilege is in each employee's own interest and that privilege reduction is happening across the organization.
- Communicate the potential for attackers to impersonate executives, partners, or customers using email spoofing, collaboration platforms, and fake social media accounts.
- Offer incentives or rewards for users and administrators when they spot and raise ways to minimize their own privileges and still accomplish their jobs (make it a challenge/game).

CYBERARK

Mitigate risk with a security-first approach to identities with the global leader in Identity Security



CYBERARK COMPLETE IDENTITY SECURITY

Security First Approach | AI Powered | Frictionless Experience | Everywhere

Provide a modern approach to Identity Security anchored on privilege to protect against advanced cyber threats. Get started today:

- Begin a trial of CyberArk Identity Security SaaS solutions
- Sign up for a demo of our Identity Security SaaS solutions today on CyberArk.com
- Get the CyberArk Blueprint Toolkit, a framework for assessing your strategy and defining a roadmap for Identity Security success

Deploy an Identity Security program

For centuries, thieves, con artists, hackers, malicious insiders, and all bad actors have relied on taking on the identity of others to achieve their impact or goal. Identity Security is a holistic approach for securing all identities to reduce cyber risk and is the foundation for a Zero Trust security strategy. This book dives into this approach and gives you actionable next steps to focus on helping your organization protect identities and ultimately safeguarding the company.

Inside...

- Defining Identity Security
- Drivers for securing identities
- Identity Security controls
- Zero Trust with Identity Security
- Launching an Identity Security program
- Reducing Identity Security risks

Aaron Pritz is an IT and security leader with 20+ years of experience in life sciences. He's a creative strategist that brings strategy to life through successful execution. He is the CEO of Reveal Risk, a boutique consulting company focused on building cyber programs with deep industry experience.

ISBN: 978-1-119-83057-3
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.