CYBERARK® | aws

WHITEPAPER

Zero Trust's Evolution: The Role of Identity Security

Practical advice for a successful Zero Trust implementation

Table of Contents

Introduction

Eighty-eight percent of security leaders agree that adopting more of a Zero Trust approach is important-to-very important.[1] But while desire is there, overall implementation is lagging.

The rapid pace of digital transformation, increased use of cloud services and adoption of hybrid work has created a continually shifting enterprise environment that's chaotic and difficult to secure. Consider these findings:

- Ransomware breaches rose 13% from 2021, representing an increase greater than the past five years combined.[2]
- Seventy-one percent of organizations suffered a successful software supply chain-related attack in the past year, resulting in data loss or asset compromise.[3]
- Meanwhile, the average cost of a data breach hit an all-time high of $4.35 million in 2022.[4]

THE THREAT OF INACTION

The reality of today's identity-focused threat landscape demands a fresh look at defense, and Zero Trust has gained popularity as a result. Built on an "assume breach" mindset and embracing a "never trust, always verify" model, this approach has emerged as the gold standard for security teams and is front-of-mind for security leaders.

Clearly, it's no longer a question of whether an organization will suffer a cyber attack but when.

Today's ever-evolving threat landscape depends on being able to continuously verify, manage and secure identities to prevent breaches. And it's crying out for an approach and controls that can help prevent and contain attacks, therefore limiting the risk of full-scale data breaches. Indeed, the Zero Trust approach has emerged as the industry standard for tackling these challenges.

Security leaders and IT teams know all of this. So, what's stopping them from Zero Trust adoption?

The short answer: it's another thing to deal with. Responding to alerts, investigating breaches and keeping the trains running amid a shortage of cybersecurity staff and skills naturally take priority. Adopting a Zero Trust strategy on top of that can feel daunting.

Even when security leaders do move forward with Zero Trust, there are three main barriers:

- How and where to start, given the scale and complexity of modern IT environments
- How to implement a Zero Trust strategy without hurting productivity
- How to gain the visibility that's needed for access to a wide variety of enterprise assets

---

[1] CyberArk, "The CISO View Survey," 2021

[2] Verizon, "Data Breach Investigations Report," 2022

[3] CyberArk, "Identity Security Threat Landscape Report," 2022

[4] IBM, "Cost of a Data Breach Report," 2022

The Path to Zero Trust Maturity

There's no silver bullet to implementing Zero Trust, given the unique demands of each organization's hybrid and multi-cloud IT projects. Yet, despite the complexities, it's become a pressing business consideration and a mindset that must be adopted across the board.

Several frameworks exist for a Zero Trust model that spans the enterprise, helping companies to chart their approach. For example, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has set out five key areas that form the foundation of Zero Trust maturity, all of which should be collectively advanced and optimized over time.[5]

These areas are:

- **Identity:** An attribute or set of attributes that uniquely describe an agency user or entity
- **Device:** Any hardware asset that can connect to a network, including Internet of Things (IoT) devices, mobile phones, laptops, servers and others
- **Network/Environment:** An open communications medium, including internal networks, wireless networks and the internet, used to transport messages
- **Application Workload:** Includes systems, computer programs and services that execute on-premises, as well as in a cloud environment
- **Data:** Includes data that should be protected on devices, in applications and on networks.

As indicated by the first of CISA's key areas, CyberArk believes organizations should focus on identity as a central tenet for creating a strong security posture. This will help enterprises navigate the barriers they face around adoption.

As such, this whitepaper explores the central role of identity in the security environment of any network, outlines five foundational principles for any Zero Trust implementation and maps out six practical steps for getting started on this journey.

THE TIME FOR ACTION IS NOW

In response to increased attacks and IT complexity, CISA has urged CEOs to act: "In this heightened threat environment, senior management should empower CISOs by including them in the decision-making process for risk to the company, and ensure the entire organization understands that security investments are a top priority in the immediate term."[6]

[5] CISA, "Zero Trust Maturity Model," 2021
[6] CISA, "Shields up," 2022

Zero Trust and Identity Security

Although enterprises had already begun their foray into digital transformation and cloud migration, the COVID-19 crisis substantially impacted how businesses operate — and the pace of change that ramped up so abruptly in 2020 has not abated.

In 2022, nearly all organizations (99%) reported fast-tracking the adoption of at least one business or IT initiative over a 12-month span.[7] Yet, rapid change meant granting more access. The number of identities multiplied significantly, and the attack surface grew with them.

In the past, privileged access was traditionally confined to a predictable pool of users (the IT and network admins of the world). Today, any identity — a workforce user, customer, third-party vendor, device, bot or application — can be a potential pathway to an organization's most valuable assets. In fact, it's thought more than half (52%) of an organization's human workforce and 68% of bot or machine identities have access to sensitive corporate data.[8]

THE GREAT IDENTITY SURGE

The majority of security incidents start with identity as the ingress point — indeed, the human element accounts for 82 percent of analyzed breaches.[9] And this threat vector continues to grow.

Business leaders may know that the growing complexity of today's enterprise underscores the importance of increased cybersecurity investment. But they don't always allocate those resources effectively. Given the threat that mismanaged or over-permissioned identities represent, unless a company makes identity the central focus of its Zero Trust strategy, its increased spending will not necessarily result in a decreased attack surface.

[7] CyberArk, "Identity Security Threat Landscape Report," 2022
[8] CyberArk, "Identity Security Threat Landscape Report," 2022
[9] 2022 Verizon, "Data Breach Investigation Report," 2022

Identity as the Central Pillar of Zero Trust

In many ways, the Zero Trust mindset was made for this moment. Serving as an end-to-end approach to enterprise resource and data security, it covers every component of today's identity surge and its security ramifications.

"Never trust, always verify" — the cornerstone of the Zero Trust philosophy — becomes especially relevant when companies examine the myriad vulnerabilities created by the entry points and pathways traversed by multiple identities. Often, these entry points are guarded by poorly protected credentials and can be accessed by identities with too much privilege.

For any Zero Trust project to be successful, identity must play a central role from the outset. It's a key pillar for all areas of Zero Trust investment, which means it must be executed well early on.

Modern Identity Security controls, centered on privilege, lay the foundation for this by limiting access to those who need it and only granting the minimum privilege for the task in question. This includes continuous authentication to validate the user's entire session — not simply a single MFA request — and monitoring user behavior to identify when an identity has been compromised.

For any Zero Trust project to be successful, identity must play a central role from the outset.

It's a key pillar for all areas of Zero Trust investment, which means it must be executed well early on. Modern Identity Security controls, centered on privilege, lay the foundation for this by limiting access to those who need it and only granting the minimum privilege for the task in question.

The Five Principles of Any Zero Trust Implementation

Every company will implement Zero Trust differently. But the foundation of any Zero Trust approach and deployment, irrespective of industry or use cases, should be grounded in a set of constants.

Zero Trust is both a mindset and a practical change, touching on all aspects of an enterprise security strategy. As such, any organization working to implement an effective approach should start by applying the following five principles to create a holistic safety framework.

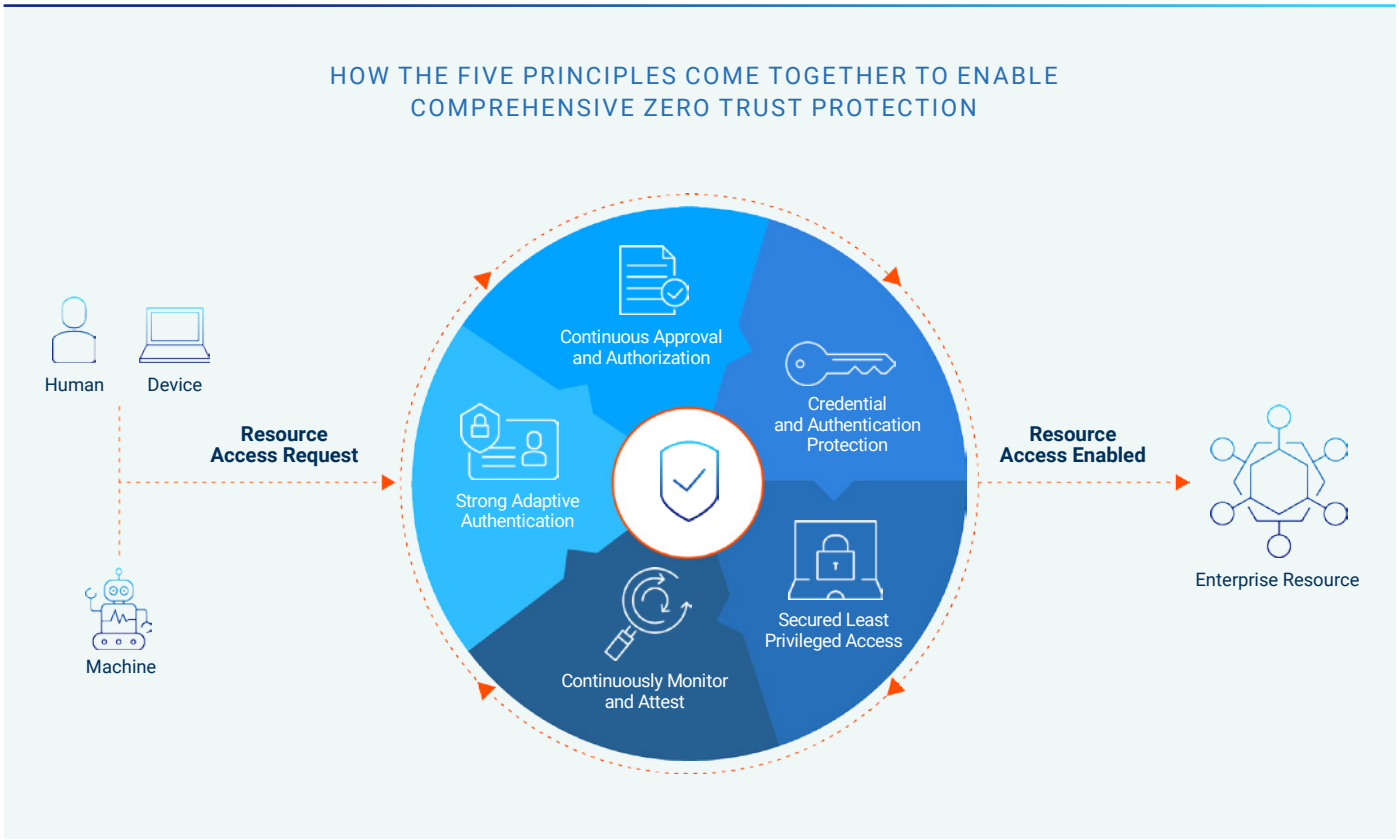


Figure 1

1. Strong, adaptive authentication

Challenge: Passwords alone are insufficient to verify a user's identity and protect the enterprise from loss, fraud or malicious attacks. Stronger, risk-based safeguards can help companies balance the conflicting needs for security and productivity.

Action: Extend an adaptive form of multifactor authentication (MFA) with intelligent risk-based access, applying context from a user behavior analytics engine that is continuously learning. This will determine parameters for typical behavior.

Real-world example: A user's last access attempt came from California. An hour later, that same identity makes an access request from London after an MFA attack. This request will be blocked, as it is not possible for the user to have made the journey in that time (unless, of course, the user has a teleportation device).

2. Continuous approval and authorization

Challenge: Relying only on authentication challenges at log in is not enough to protect against today's sophisticated types of attacks.

Action: Revalidate user identities to ensure they should have access and reauthenticate for sensitive actions or after periods of inactivity.

Real-world example: A user accessing a sensitive business application, such as a payment processing system, can be authorized at log in and then issued another challenge when they navigate to sensitive parts of the app or perform high-risk actions. The same approach can work for staff who use a shared workstation to access sensitive data.

3. Secured least privilege access

Challenge: Enterprises need to intelligently limit excessive access to their hybrid and multi-cloud resources. Then, they must secure the access itself. Once an identity has been authenticated and approval given, the system should grant access in the least privileged way.

Action: Adopt a least privilege stance. Provide only the permissions needed to perform a specific task. When possible, elevate privileged access just in time; then remove permissions when the task is complete. This reduces the risks of compromised standing access. Proactively analyze entitlements to access sensitive resources and remove excessive permissions, especially in public cloud environments where they can rapidly accumulate.

Real-world example: Third-party vendor identities receive elevated access in real time to perform a certain function, such as executing tasks or programs that need admin rights. In this situation, access can be elevated temporarily and authorized via MFA.

THE RISK OF EXCESSIVE PERMISSIONS

Across AWS, Azure and GCP, there are now more than 30,000 possible permissions that can be assigned to a human or machine identity.[10] And many of the identities with these permissions also have access to SaaS apps or on-premises resources. These excessive permissions pose significant risk as organizations pursue Zero Trust frameworks calling for every identity attempting to access corporate resources to be verified and their access intelligently limited.

4. Continuously monitor and attest

Challenge: Just as privilege is not binary, neither are access decisions. Enterprises must adopt continuous monitoring to confirm that what is happening should be happening and detect anomalies as they arise.

Action: Analyze behavioral patterns among end users, apply risk scoring and continuously monitor access to create a feedback loop that informs subsequent access decisions, providing the context to adapt controls on the fly.

Real-world example: Monitor the work sessions of any user who is accessing a sensitive business application. All actions are recorded after a user is logged in, creating an audit trail that gives more context for future authentication and continuous approval considerations.

5. Credential and authentication protection

Challenge: Endpoint-originating attacks can be devastating. Bad actors will look to circumvent controls and find their way around additional security layers such as MFA.

Action: Block credential theft at the endpoint to counteract identity-based vulnerabilities. Put automated detection controls in place to detect and block credential theft attempts via software abuse or memory scraping.

Real-world example: Protecting credentials stores and authentication caches on the workstation mitigates the endpoint attack vector. Authenticate all attempts to escalate privileges at the endpoints.

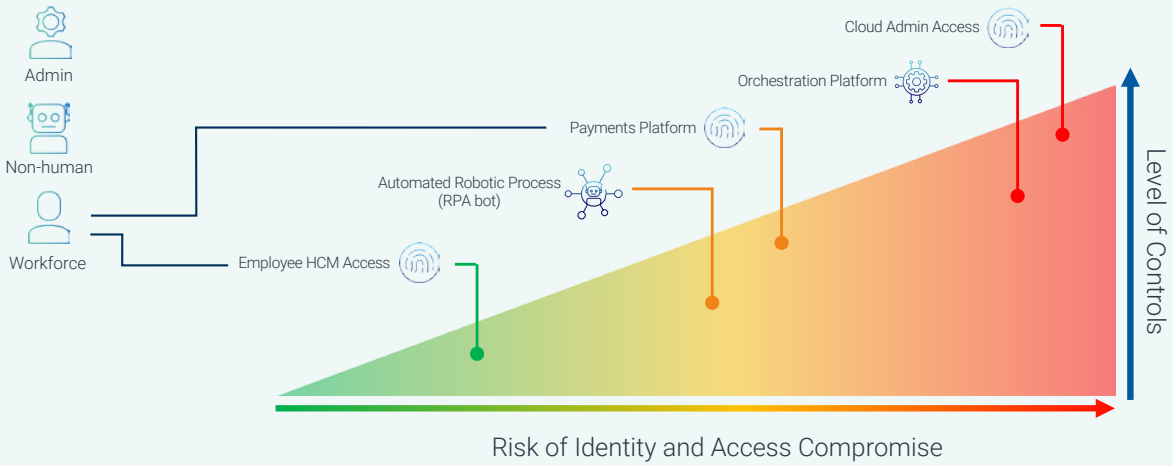
[10] CyberArk Cloud Entitlements Catalog, August 2022

CONTROLS BASED ON EACH IDENTITY'S RISK PROFILE

Setting up appropriate Identity Security controls based on the risk profile of each identity is critical. Consider the substantial level of access the average workforce user now has. Figure 2 shows how a company can approach risk controls for different identities based on the resources they're accessing and the inherent risk of that access.

A RISK-BASED APPROACH TO SECURING ACCESS

Deliver a unified platform that enables organizations to implement the relevant controls in relation to the associated risk



Envision a scenario in which a workforce user from the finance team performs a routine activity such as going into the HR system to request time off. Next, the user moves on to access the enterprise's payment system — as part of their role — gaining access to organization-wide employee salary data. Each type of access requires a different form of control relevant to the potential risk. On the flip side, putting too many security controls on a less-risky type of access could lead to wasted investments and a negative impact on user experience.

Figure 2

Six Focus Areas for Getting Started with Zero Trust

Enterprises can use the aforementioned five principles to create a solid foundation for building a robust Zero Trust architecture. With a good grasp of the principles, organizations can put them into action. From here, we'll describe the practical steps to take, in the context of six key focus areas.

Although this may seem daunting, getting started with Zero Trust is often neither as difficult — nor as expensive — as businesses may think. Not all six areas require additional investment in new technologies, meaning organizations in many cases can start their journey with what they already have. Building on CyberArk's experience in protecting identities and securing compromised environments, these six areas are a launch point for implementing a Zero Trust strategy to strengthen the enterprise security posture without impacting productivity.

Here are the six focus areas, as well as our recommendations for solutions designed to mitigate each specific threat and protect the enterprise from compromise.

1. Protect the Zero Trust architecture

The "assume breach" mindset presumes malicious actors will aim to take an organization's Zero Trust controls offline. Attackers may try to compromise access to the consoles and the network configurations of the security technologies an organization puts in place to enable a Zero Trust approach. Therefore, it's critical to implement privilege controls that can prevent attackers from taking actions such as gaining access or shutting down access entirely. Enforcing the five Zero Trust principles outlined earlier in this piece is key to ensuring the integrity of security controls that exist to protect the environment. This includes fundamentals such as securing privileged access and implementing MFA.

Example: Deploy Identity Security controls for all aspects of access to the Zero Trust components, services and processes. Secure privileged access to both administrator portals and networking components of the technologies used to implement Zero Trust Network Access and network segmentation.

Related CyberArk Solutions: Centered on intelligent privilege controls, CyberArk's **Identity Security Platform** is designed to seamlessly secure access for all identities and flexibly automate the identity lifecycle. This is paired with continuous threat detection and prevention, creating a unified approach that's built for the dynamic enterprise. Privileged access to admin consoles and underlying infrastructure can be restricted, isolated and monitored via **CyberArk Privileged Access Manager** and thoroughly authenticated with **CyberArk Identity Adaptive Multifactor Authentication**.

2. Protect authentication origins

Compromised endpoints can be used by attackers to bypass strong authentication. As such, it's essential to put controls in place that ensure only approved processes can access credential stores. This relies on the basic hygiene of implementing least privilege and removal of local admin rights at the endpoint.

Example: Orchestrate and automate all aspects and processes related to the secure use of credentials by applications and scripts, protecting the enterprise without impacting productivity.

Related CyberArk Solutions: CyberArk Endpoint Privilege Manager enforces least privilege access and strengthens application controls, so only approved processes can access authentication sources. This is designed to prevent malicious actors from gaining access to sensitive areas of the network.

3. Secure access into applications

The first two principles of Zero Trust — strong, adaptive authentication and continuous approval and authorization — provide the basis for securing workforce access to applications. This shift from network controls to identity controls creates a better user experience and boosts productivity.

Example: Implement an adaptive form of MFA that goes beyond the binary. Leverage User Behavior Analytics (UBA) to gauge whether a user's behavior merits additional or more complex authentication factors.

Related CyberArk Solutions: CyberArk Workforce Identity solutions (spanning Single Sign-On, Adaptive Multifactor Authentication, Workforce Password Management and more) are designed to create a continuous, multi-layered fabric of protection that grants access to your workforce while keeping out attackers.

4. Secure business-critical application access

Protecting and monitoring sessions — of both privileged and workforce users with high-risk access — increases overall visibility around high-value business applications. Administrators can implement secure controls without adding complexity, regardless of network location.

Example: Continuously record, monitor and audit end-user actions in web-based business applications that pose risks. Session monitoring parameters are determined by the sensitivity of the resources to which the user has access, and with which the user might be able to perform actions. This provides visibility into the sources of potential security events, from malicious or inappropriate behavior to honest (yet consequential) mistakes.

Related CyberArk Solutions: CyberArk Identity Secure Web Sessions gives visibility into every user action via session monitoring and a step-by-step audit trail, while applying continuous authentication — all without hampering productivity.

5. Secure all non-human access requests

The "never trust, always verify" mantra of Zero Trust must encompass both human and non-human identities. The recent surge in machine identities — in the form of automated DevOps tools, workflows and more — has led to non-human identities outnumbering their human counterparts by 45 to one.[11] All calls from these machine identities seeking access to network resources should be protected and secrets managed appropriately.

Example: Improve operational efficiency by enabling credentials to be centrally managed, automating secure retrieval and granting of credentials to bots and applications, so they can perform the necessary task.

Related CyberArk Solutions: CyberArk Secrets Manager protects credentials used across the DevOps pipeline, helping ensure a frictionless experience for developers and driving business agility. CyberArk also offers several other DevSecOps solutions for protecting access to sensitive resources without burdening developers.

6. Align privileged access management to Zero Trust principles

Privileged access must track with the five Zero Trust principles discussed earlier. This allows enterprises to move away from long-standing high levels of privileged access to a more dynamic, just-in-time method for administrator access. Additionally, access should be granted with minimal permissions to reduce the attack surface and blast radius, should a privileged account be targeted by malicious actors.

Example: Remove standing admin rights and enforce on-demand elevation of privilege within sessions. Ensure the admin user's workstation is protected, and all access is validated and approved at the point of access request. Isolate sessions to critical resources as an extra security layer, helping to prevent the spread of malware.

Related CyberArk Solutions: CyberArk Cloud Entitlements Manager detects and removes excessive permissions to implement least privilege access in the cloud. This analysis positions organizations to further reduce unnecessary standing access by elevating access just in time. CyberArk Dynamic Privileged Access provides admins just-in-time administrative access to virtual machines and servers, while CyberArk Secure Cloud Access grants engineering teams just-in-time access to the cloud management layer for performing environment changes. With additional support for strong authentication — leveraging a wide range of authentication methods — CyberArk offers a variety of products and solutions for building a robust Zero Trust architecture aligned with the five key principles.

[11] CyberArk, "Identity Security Threat Landscape Report," 2022

How the CyberArk Identity Security Platform Enables Zero Trust

Enterprises need an outcome-driven solution to help them implement Zero Trust successfully. CyberArk's Identity Security Platform applies intelligent privilege controls across the board to all types of identities.

This offers businesses a means to balance their security concerns with their need for operational efficiency. It's an Identity Security-based approach to keeping attackers at bay by applying protection to key areas of vulnerability, simplifying IT workflows and hardening endpoints, while enabling the enterprise to drive its digital initiatives forward.

This holistic approach to Identity Security enables an organization's Zero Touch architecture by:

1. Enforcing least privilege and securing access for humans and machines across any device, anywhere.
2. Introducing intelligent privilege controls — and infusing them across the board — to help isolate and stop attacks, protect critical assets and grant access for just the right amount of time.
3. **Automating management of the identity lifecycle** through seamless, no-code app integrations and workflows, taking control of excessive permissions to enforce least privilege.
4. Continually monitoring for threats so enterprises can adjust controls based on risk.

Figure 3 shows how various CyberArk solutions come together to deliver on this goal.

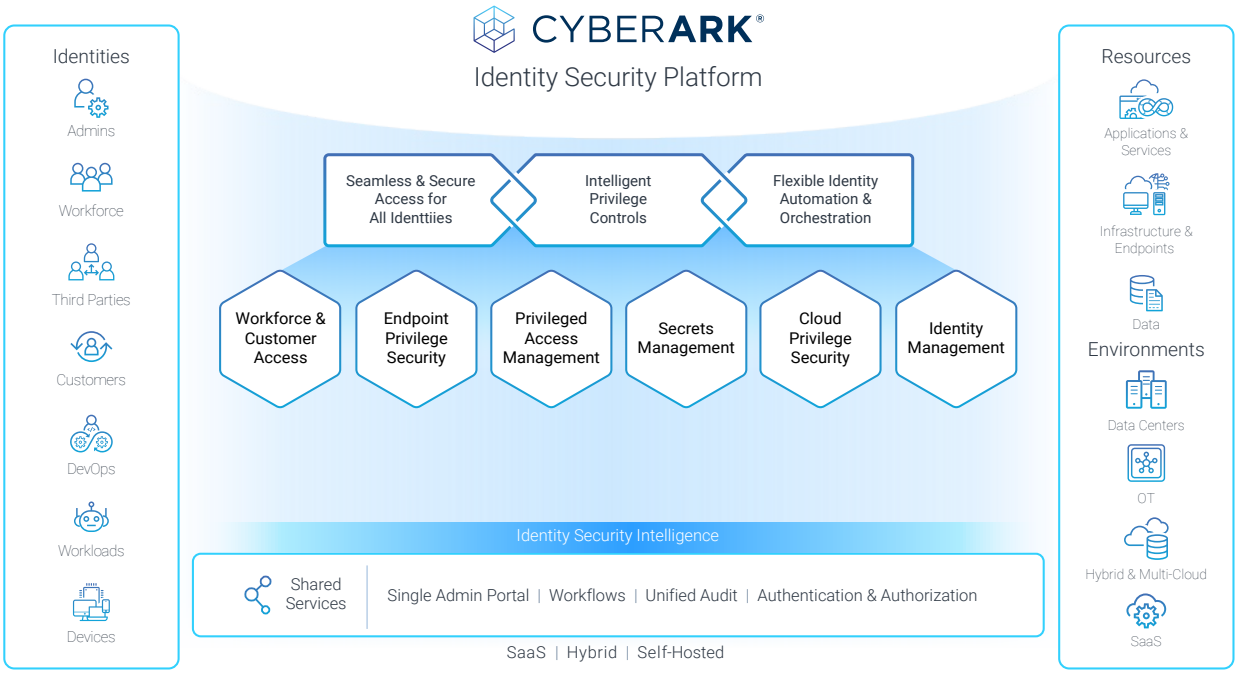


Figure 3

Ensuring the essential components (as shown in figure 3) are part of an organization's guideposts for a holistic Zero Trust approach will help a company reap the business benefits of Identity Security. Other than the most obvious — the significant reduction of cyber risk to the company — these benefits include driving operational efficiency, enabling the continued flow of the digital business and satisfying audit and compliance requirements.

Learn more about how the CyberArk Identity Security platform can help your organization **secure all identities with end-to-end protection**.

CYBERARK BLUEPRINT: A FRAMEWORK FOR IDENTITY SECURITY SUCCESS

Identity is at the heart of Zero Trust, and Identity Security gives organizations the peace of mind they need to protect their critical assets. But we understand that tackling the problem of today's identity surge and its inherent risks can seem daunting. To help you get started, the **CyberArk Blueprint for Identity Security Success** offers a best-practice framework for securing the ever-expanding number of identities a modern enterprise needs to deal with.

The Blueprint includes:

- Guidance for developing a successful Identity Security program or initiative across your company's people, processes and technology domains.
- A structured, risk-based approach to reduce risk in a measurable way.
- Areas of importance to implement change quickly and efficiently, ensuring a rapid return on your security investments.

Built on CyberArk's collective experience in the Identity Security space — gathered from more than two decades of lessons learned through working with 7,500 global customers and more than half of the Fortune 500 — the Blueprint covers the full scope of human and non-human identities.

Conclusion

We've all heard the adage that those protecting themselves must be successful 100% of the time, whereas an attacker only needs to be successful once. And that's why Zero Trust plays such an important role in the enterprise armory.

Zero Trust is neither a quick fix nor straightforward to adopt, and its implementation can be complex. But the exponentially increasing number of identities to be managed — and the threat each identity can represent — highlights the urgent need for enterprises to adopt a Zero Trust mindset.

An identity-based approach to Zero Trust is growing in popularity for good reason. Identity Security is the means to achieve measurable risk reduction and speed up the implementation of Zero Trust frameworks. By securing routes to critical assets or underlying administrative access, establishing strong adaptive authentication and removing hard-coded secrets, enterprises using an Identity Security-based approach to underpin their Zero Trust framework can dramatically improve their overall security posture.

About CyberArk

CyberArk is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets.

CYBERARK®