



CYBERARK[®]
The Identity Security Company

WHITEPAPER

Addressing Zero Trust for Government: The Role of Identity Security

Practical advice for a successful transition to Zero Trust

Table of Contents

Introduction	3
The Barriers to Zero Trust	4
The Path to Zero Trust Maturity	5
Zero Trust and Identity Security	6
Identity as the Central Pillar of Zero Trust	7
The Five Identity Security Principles of Any Zero Trust Implementation	8
Six Identity Security Focus Areas for Getting Started with Zero Trust	12
How the CyberArk Identity Security Platform Enables Zero Trust	15
Conclusion	17

Introduction

Governments around the world are enacting stronger cybersecurity mandates in which Zero Trust features as a central theme. Eighty-eight percent of security leaders agree that adopting a Zero Trust approach is very important.¹ But while desire and regulatory momentum is there, overall implementation is lagging.

Major shifts are converging to create a proliferation of identities and, in turn, a chaotic environment that is difficult to secure. A key example: the rapid pace of cloud and digital transformation initiatives, paired with a still ongoing dependency on legacy IT. Add in factors such as governments' growing employment of contractors and the adoption of hybrid work, and you end up with an attack surface free of boundaries and rife with vulnerabilities. Consider these findings:

- Ransomware attacks increased 13% from 2021, comprising up to 25% of all breaches in 2022.²
- Ninety-five percent of organizations reported a backdoor software supply chain attack, which will likely only get worse as enterprises rely on more third parties.³
- Meanwhile, the average cost of a data breach hit an all-time high of \$4.35 million in 2022.⁴

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.

THE ISSUE OF TECHNICAL DEBT

Digital transformation takes time. Whilst governments continue to modernize IT, legacy systems cost significant funds to maintain and often extend the risk surface through their inherent security vulnerabilities. In 2019, the UK public sector spent close to 50% of its \$5.76 billion IT budget on maintaining outdated systems.⁵ In 2021, most of the US government's \$100 billion spent on technology went towards operating and maintaining legacy technologies.⁶

¹ CyberArk, "[The CISO View Survey](#)," 2021

^{2,3} Verizon, "[Data Breach Investigations Report](#)," 2022

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

⁵ Britain's Digital Economy Council, "[Organizing for Digital Delivery](#)," 2020

⁶ U.S. Government Accountability Office, "[Agencies Need to Develop and Implement Modernization Plans for Critical Legacy Systems](#)," 2021

REGULATORY MOMENTUM FOR ZERO TRUST

In the spring of 2021, the White House issued an executive order putting into place guidelines on how to improve the nation's cybersecurity stance. This requires U.S. federal agencies to modernize their approach to cybersecurity by becoming more transparent about cyber threats for protection. Government agencies are required to move toward a Zero Trust architecture, incorporating guidelines from the National Institute of Standards and Technology (NIST).

Flash forward to 2023, whilst not universally applied outside of the U.S., NIST has become a reference framework for governments globally. With its new and improved Network and Information Security Directive, NIS2, the European Union additionally joins the US with a stronger cyber security mandate promoting Zero Trust principles which will next be folded into country-specific laws, such as KRITIS in Germany, CAF in the UK and the rules governing Opérateurs de Services Essentiels (OSE) in France.

The Barriers to Zero Trust

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

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 assets

The global cybersecurity workforce shortage widened in 2022 by 26.2% to reach a staggering 3.42 million people⁷

⁷ISC2, [Cybersecurity Workforce Study, 2022](#)

The Path to Zero Trust Maturity

There's no silver bullet to implementing Zero Trust, given the unique demands of government agencies. Yet, despite the complexity, it's become a pressing consideration and a mindset that must be adopted across all levels of government.

Several frameworks exist for a Zero Trust model, helping organizations 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.⁸

These areas are:

- **Identity:** An attribute or set of attributes that uniquely describe a government 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 government agencies 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, the Cybersecurity and Infrastructure Security Agency (CISA) has urged leaders 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."⁹

⁸ CISA, "[Zero Trust Maturity Model](#)," 2021

⁹ CISA, "[Shields up](#)," 2022

Zero Trust and Identity Security

Although governments had already begun their foray into digital transformation and cloud migration, the COVID-19 crisis substantially impacted how agencies 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.¹⁰ Yet, rapid change meant granting more access. The number of identities multiplied significantly, and the attack surface grew with them. Indeed, 77% of government organizations (excluding public healthcare) and 92% of healthcare organizations (public and private) believe it's somewhat-to-highly likely that new digital services for citizens could result in increased security risks or cyberattacks.¹¹

In the past, privileged access was traditionally confined a predictable pool of users (the IT and network admins of the world). Today, any identity – a member of staff, member of public, third-party vendor, device, bot or application – can be a potential pathway to an entity's most valuable assets. In fact, it's thought more than half (52%) of an organization's (IT) users and 68% of bot or machine identities have access to sensitive data.¹²

THE GREAT IDENTITY SURGE



The majority (80%) of security incidents start with identity as the ingress point, in the form of compromised credentials.¹³ And this threat vector continues to grow. Cloud-first mandates and other digital initiatives have more than doubled the number of identities to be managed, according to 85% of security stakeholders. Of those, 95% say they find the task of managing those identities to be a challenge.¹⁴

Management may know that growing complexity 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 an organization makes identity the central focus of its Zero Trust strategy, its increased spending will not necessarily result in a decreased attack surface.

^{10, 11, 12} CyberArk, "[Identity Security Threat Landscape Report](#)," 2022

¹³ 2022 Verizon, "[Data Breach Investigation Report](#)," 2022

¹⁴ CyberArk, "[Identity Security Threat Landscape 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 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 organizations 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 transition 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 challenge offered through a conventional MFA tool — and monitoring user behavior to identify when an identity has been compromised.



THE DOD COMMITMENT TO ZERO TRUST

The US largest government agency, the Department of Defense (DOD), has adopted a 'Zero Trust Strategy and Roadmap' with the goal to transition to a Zero Trust architecture by (fiscal year) 2027. It stipulates four overall objectives:

- 1. Zero Trust Cultural Adoption.** All DOD personnel understand and are aware, trained, and committed to a zero-trust mindset and culture to support integration of Zero Trust.
- 2. DOD information Systems Secured and Defended.** Cybersecurity practices incorporate and operationalize Zero Trust in new and legacy systems.
- 3. Technology Acceleration.** Technologies deploy at a pace equal to or exceeding industry advancements.
- 4. Zero Trust Enablement.** Department- and component-level processes, policies, and funding are synchronized with Zero Trust principles and approaches.

¹⁵ U.S. DOD, "Department of Defense Releases Zero Trust Strategy and Roadmap", 2022

The Five Identity Security Principles of Any Zero Trust Implementation

Individual government agencies will implement Zero Trust differently. But the foundation of any Zero Trust approach and deployment, irrespective of level of government 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 a cyber 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 – and even standard MFA tools that can't evaluate the context of a high-risk log-in – alone are insufficient to verify a user's identity and protect the entity from loss, fraud or malicious attacks. Stronger, risk-based safeguards can help governments balance the conflicting needs for security and productivity.

Approximately 40% of the US Federal government workforce consists of contractors¹⁶ and one of their biggest challenges is to remove inappropriate access during the digital modernization process. Challenges moreover persist when extending that scope beyond staff and contractors – the UK government currently offers more than 190 ways citizens can access their GOV.UK services¹⁷; over time they want to consolidate this to a single, simple and secure access route.

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.

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 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: Government agencies 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. Many government agencies have administrative overhead issues associated to provisioning and de-provisioning access; it can take days or weeks for staff incl. contractors to gain access to required, critical, apps and services.

¹⁶ Volcker Alliance, "The True Size of Government," 2017

¹⁷ GOV.UK Government Digital Service, "One Login for Government: December 2021 update," 2021

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 an adaptive form of MFA.



SECURING ACCESS FOR CONTRACTORS AND THIRD PARTIES

Many third-party identities that can access sensitive government resources – for example, through using SaaS applications – also require comprehensive protection, even when they don't fall under the traditional definition of privileged users. Here, adaptive MFA can secure external identities as part of a defense-in-depth approach that also includes automated lifecycle management processes.

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.¹⁸ 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 government 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. Government agencies 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 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.

¹⁸ CyberArk Cloud Entitlements Catalog, August 2022

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.

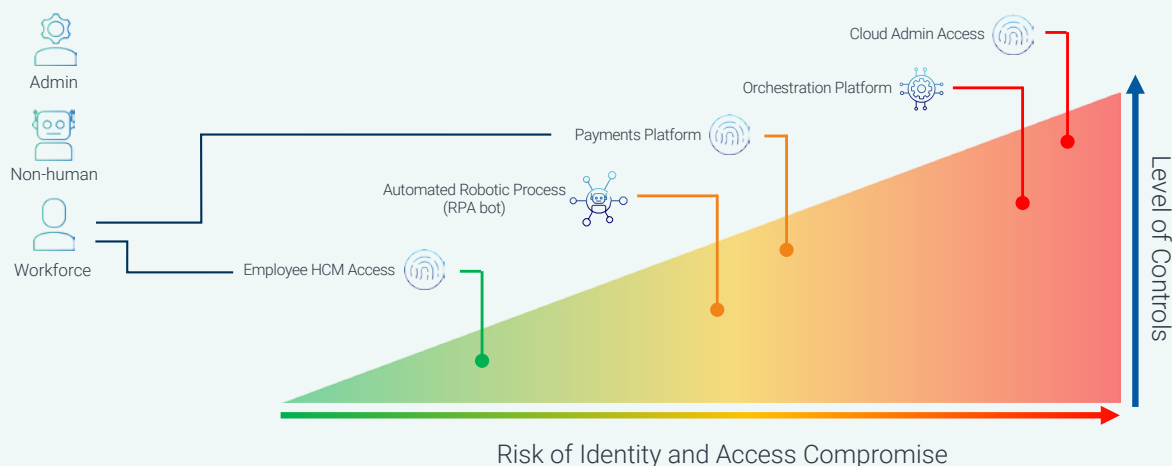


CONTROLS BASED ON EACH IDENTITY'S RISK PROFILE

Setting up appropriate Identity Security controls based on the risk profile of each identity is critical. Consider the substantial level of access an average member off staff now has. Figure 2 shows how an organization 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 member of staff from the finance team performs a routine activity such as going into the HR/ payroll 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 staff 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 Identity Security Focus Areas for Getting Started with Zero Trust

Government agencies can use the aforementioned five principles to create a solid foundation for building a robust Zero Trust architecture. With a good grasp of these 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 one may think. Not all 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 areas are a launch point for implementing a Zero Trust strategy to strengthen the 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 organization 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, the [CyberArk 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. 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 organization 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 staff 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 members of staff the access they need, while keeping malicious actors out.

4. Secure business-critical application access

Protecting and monitoring sessions — of both privileged and regular staff users with high-risk access — increases overall visibility around high-value 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 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 (respectively also referred to as ‘PE’, Person Entities and ‘NPE’, Non-Person Entities). 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.¹⁹ 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 government agencies 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.

¹⁹ CyberArk, “Identity Security Threat Landscape Report,” 2022

How the CyberArk Identity Security Platform Enables Zero Trust

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

This offers organizations 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 organization to drive its digital initiatives forward.

This holistic approach to Identity Security enables a government agency's Zero Touch architecture by:

1. Enforcing least privilege and seamlessly securing access for humans and machines across any device, and any environment from hybrid to multi-cloud.
2. Applying intelligent privilege controls to every form of identity — human and machine — 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 through real-time Identity Security intelligence, so organizations can adjust controls based on risk, and leverage real-time remediation options.

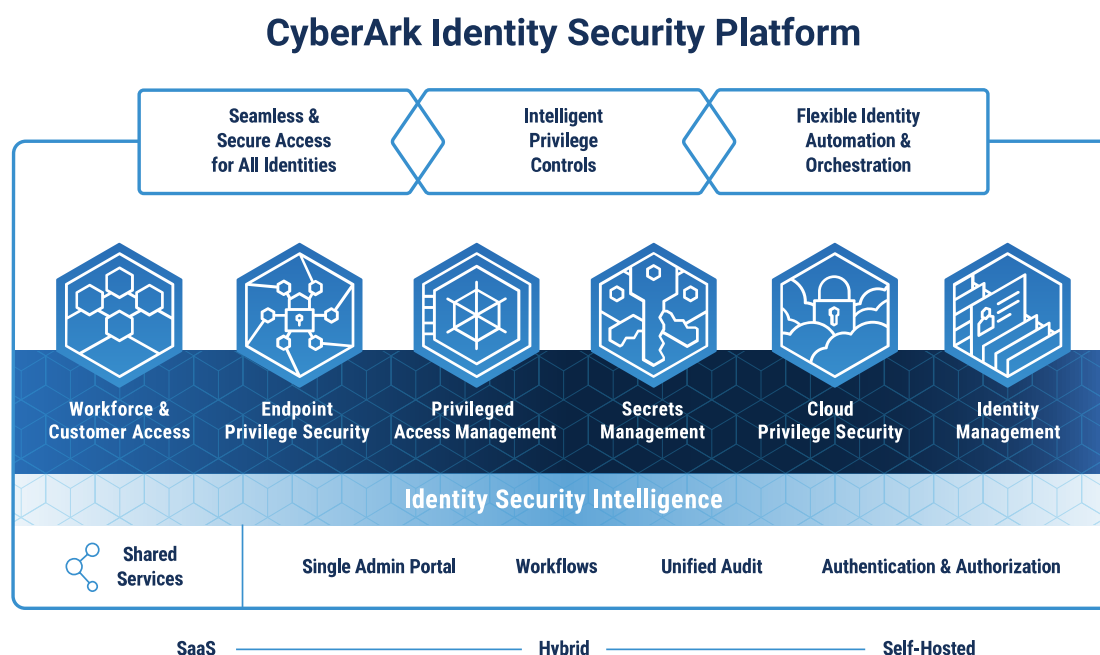


Figure 3

Figure 3 shows how various CyberArk solutions come together to deliver on this goal. Ensuring these essential components are part of an organization's guideposts to setting a holistic Zero Trust approach will help agencies reap the benefits of Identity Security. Other than the most obvious — the significant reduction of cyber risk — these benefits include delivering operational efficiencies, securing digital transformations and helping satisfy 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 governments need 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 more than 8,000 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.

Although transitioning to Zero Trust may seem daunting, getting started is often neither as difficult — nor as expensive — as one may think. Ultimately, the exponentially increasing number of identities to be managed — and the threat each identity can represent — highlights the urgent need for governments to adopt a Zero Trust mindset.

- An average member of staff accesses more than 30 applications and accounts²⁰
- Machine identities outnumber human identities by a factor of 45x²¹
- 52% of all staff identities have access to sensitive systems and data²²

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, government agencies using an Identity Security-based approach to underpin their Zero Trust framework can dramatically improve their overall security posture.

^{20, 21, 22} CyberArk, "[Identity Security Threat Landscape Report](#)," 2022

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.



©Copyright 2023 CyberArk Software. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners.

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice. U.S., 03.23 Doc. TSK-2948

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