Deloitte.

CYBERARK

Protecting your most critical assets starts with **Identity Security**

September 2023

Protecting your most critical assets starts with **Identity Security**

In today's world, organisations are becoming more interconnected than ever before. They are digitising their processes and enabling their workforce to access critical assets remotely. As the number of digital touchpoints between the workforce and critical digital assets increases, the need for security over access to these assets becomes imperative to secure your organisation’s growth.

Deloitte Switzerland and CyberArk have helped numerous clients to secure their digital assets through Identity Security. Our partnership and leading market position have given us valuable insights into the common challenges and pitfalls faced by customers. We would like to share some of these insights to guide you in establishing Identity Security to protect your critical assets.

Discover the key industry trends and lessons learned in this article.

Securing your most critical assets

CHALLENGE

Unmanaged privileged accounts are often targeted by cyber criminals to gain access to your organisation's critical assets to insert malware, spyware, or to impact your day-to-day operations. In today's complex and interconnected systems it is increasingly difficult to enforce controls and ensure auditability of access to critical data and infrastructure. As such, it is key to protect your most critical assets from both internal and external threats.

BUSINESS DRIVERS

- **Defend your brand reputation** by protecting against internal and external attacks through discovery and monitoring, segregation of duties, and least privilege access to prevent and detect misuse of identities.
- **Demonstrate regulatory compliance** during audits through automated monitoring and reporting, central visibility, policy enforcement and segregation of duties.
- **Enhance user experience** by establishing frictionless onboarding processes for all identity types including your customers, partners, employees and external contractors.
- **Securely manage remote access** for external users requiring access to critical assets, to improve control over your third party risks.
- **Enforce User accountability** through clear traceability of activities to a single user (external or internal)

OUR IMPACT

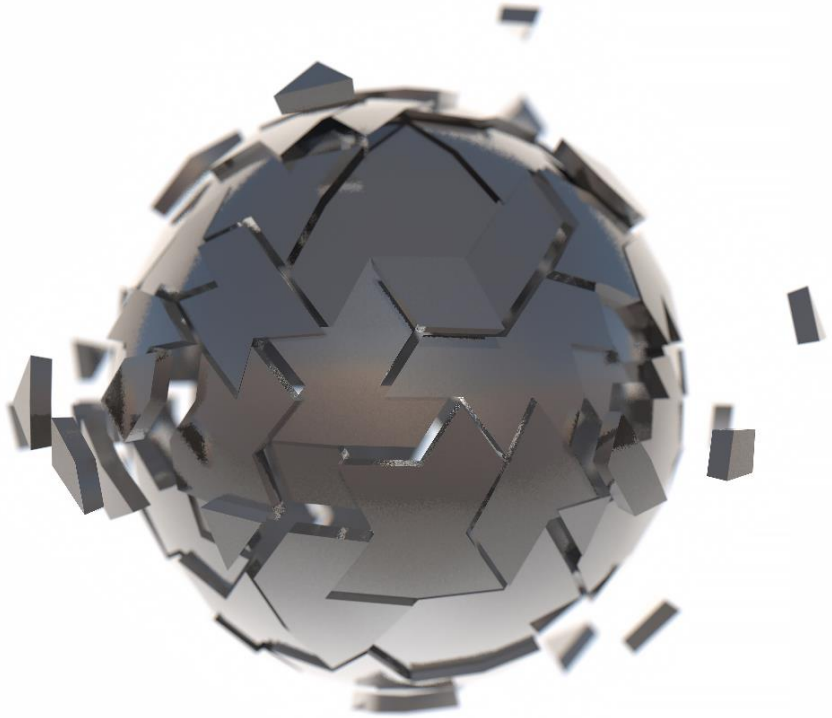
Deloitte Cyber brings 20+ years of experience across all areas of Identity and Access Management to help clients sustain, transform, and evolve their identity capabilities. Through our partnership with CyberArk, we offer clients direct added value with proven frameworks and best practices as well as technical expertise to support clients in implementing Identity Security solutions.

Industry insights

As implementation partner for clients in various business sectors, Deloitte finds itself in a unique position where we see what is happening across industries We notice some key trends that can help cyber security leaders and decision makers to ensure that their organisation is secure

KEY INDUSTRY TRENDS

1. **Zero Trust**. Zero Trust is an IT security model that requires all users, devices and applications to authenticate and verify themselves before being granted access to an organisation's resources on a need to know basis. Identity security solutions help you achieve a zero trust model, for example: Administrative activities on critical assets can be monitored and secured through session isolation techniques provided by privileged access management (PAM) solutions.
2. **Securely managing machine identities**. Efficient management of secrets in the CI/CD pipeline, services, scripts, and code is increasingly important considering only 25% of sensitive access to bots and robotic process automation (RPA) is adequately secured[1]. Integrating Identity Security solutions into the DevOps workflow can make it easier to manage privileged access and credentials across the organisation.
3. **Securing OT access**. With 62% of security teams operating with limited visibility[1], monitoring access to OT such as production lines and critical infrastructure, is crucial for overall OT security. Identity Security solutions help in securing remote access to OT environments, monitoring for irregular behaviour and enforcing a layered security architecture.
4. **Cloud is on the rise**. As organisations adopt cloud based services, with an expected increase of 68% in SaaS tools deployed over the next 12 months[1], cloud based Identity Security solutions are gaining popularity. While cloud based solutions offer greater flexibility, scalability and cost-efficiencies, organisations should not overlook their on-premises footprint as threat surface.
5. **Growing regulatory requirements**. With the implementation of regulations such as DORA, FINMA, NIS 2, organisations face increased pressure to demonstrate compliance in security controls. These regulations impose stricter security requirements, making compliance a top priority for organizations.



[1] Source: 2023 Identity Security Threat Landscape Report, CyberArk

Lessons learned

Implementing an effective Identity Security solution requires a comprehensive approach that involves multiple stakeholders and encompasses various phases. Find out below some of the key considerations if you are looking to implement or enhance Identity Security in your organisation

KEY CONSIDERATIONS

1. **Involve the right stakeholders.** As part of an Identity Security programme, it is essential to involve business representatives along with your IT teams. Securing privileged access requires working with application owners, IT platform teams (e.g., Linux, Windows, directory services, etc.), and compliance and risk teams, to capture the right set of business requirements.
2. **Start with strategy and governance.** Develop a comprehensive Identity Security strategy along with a target operating model, including but not limited to policies, processes, and technology solutions, to avoid the need for reworking later in the implementation phase.
3. **Plan for change.** Develop a training programme to ensure that end-users are properly trained to use the solution, reducing the required effort for awareness and operational support. Inform users by providing demo sessions in different time zones, offer tailored training materials, and nominate change champions for service lines or business units. Identity Security solutions are often misunderstood and may come across as complex, so communication and training is essential to reduce complexity for end users.
4. **Risk-based rollout approach.** Begin by prioritising your most critical systems and identities during the rollout. While it is common to prioritise specific use cases based on perceived importance, conducting a thorough business impact assessment and identifying your crown jewels enables you to prioritise use cases objectively.

Contacts and authors

Deloitte AG

Reto Haeni
Partner – IAM, Infrastructure and Cloud Security
+41 79 345 01 24
rhaeni@deloitte.ch

Ashish Gupta
Senior Manager - IAM Service Lead
+41 79 898 90 32
asgupta@deloitte.ch

CyberArk Software Ltd.

Marcel Beil
Account Executive
+41 79 400 82 39
marcel.beil@cyberark.com

Olivia Rey
Channel Account Manager – Switzerland and Austria
+41 79 335 27 88
olivia.rey@cyberark.com