IDC VENDOR SPOTLIGHT

Sponsored by BeyondTrust

This paper examines the need for identity-focused security in Africa. It highlights the digital adoption trends that lead to vulnerable business postures and delves into methods to enhance security strategies using privileged controls. The paper's aim is to help establish a sound privileged access security strategy road map for Africa.

Africa's Road Map to Identity Maturity and Security Using Privileged Access Controls

October, 2023

Written By: Associate Research Director Shilpi Handa, Cybersecurity, IDC

Africa: A Soaring Need for Identity Security

In an evolving integrated world, robust and resilient cybersecurity is a nonnegotiable prerequisite for growth in any economy. In the last few years, Africa has seen increasing IT investments to boost digitalization. In July 2023, IDC's Worldwide Black Book Live Edition reported that total IT spending on the continent is projected to reach $36.2 billion in 2023, representing a compound annual growth rate (CAGR) of 6.4% over the 2021–2026 period.

But effective cybersecurity remains a challenge across Africa. Many organizations are still unprepared for potential cyberattacks, and only a handful of countries have cybersecurity regulations in place to protect consumers and businesses.

Interpol's *African Cyberthreat Assessment Report 2021* found that more than 90% of businesses on the continent were operating without the minimum necessary cybersecurity protocols. The threat is not confined to business. Digital extortion, online scams, and phishing are increasingly targeting individuals. The Interpol report states: "According to African member countries, the most prevalent and pressing cyberthreat is online scams." Banking and credit card fraud is also recognized as a serious threat. Such crime involves the theft of personal data and/or banking details, which are then used by the threat actor to purchase goods or siphon funds from personal accounts. Sometimes, the stolen personal details are sold on illicit markets for use by other criminals.

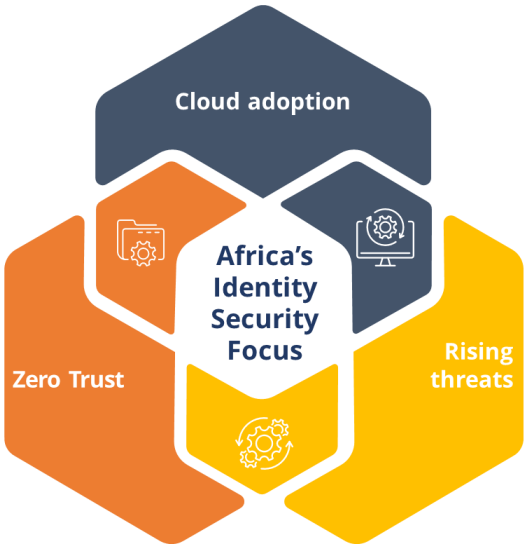
Not only are companies and their employees vulnerable to cyberthreats, but *individual identity* itself is at risk from cyberattack in Africa today.

Yet this reality has not caught up with most African organizations. According to IDC's July 2023 Worldwide Security Spending Guide, expenditures on identity and digital trust software were $92.2M in 2022, or just 9.2% of the total security software spending in South Africa and the rest of the Middle East and Africa. The lion's share of spending still goes to endpoint and network security.

When embarking on a digital transformation journey (e.g., cloud first, application outsourcing, and remote working), organizations often neglect to transform their cybersecurity practices. As IT needs evolve, so must the means of securing them. New ways of working — remote work, BYOD, cloud, and software as a service (SaaS) — have fundamentally changed network perimeters. As the physical demarcation of network perimeters expands, organizations should focus on creating identity-based perimeters and access-based boundaries.

Privileged access and identity security represent a journey rather than a single solution. Because implementing such protection can be complex, IDC recommends that African organizations start by securing the crown jewels — the most privileged users — and slowly build identity maturity from there.

A Growing Need for "Access-Based Boundaries"



Over the last few years, the cybersecurity industry has unanimously sought to persuade organizations to modify their perceptions of their perimeters. Many organizations use IP-based address identification to control application access. But, as organizations adopt cloud, increase reliance on third-party SaaS, and prioritize employee flexibility via remote work strategies, an IP-based identification perimeter becomes less effective.

With no fixed network boundary and rising numbers of users, organizations may lose track of access controls and privileges, especially in hybrid environments. Hence the need for privileged access, which should apply to administrators as well as a much wider group within the enterprise and beyond. Because privileged accounts have more authority and access to resources, they are the most lucrative threat vector for many attackers. Ignoring the need to establish privileged access can lead to significant security failures and losses.

The key role of privileged users is illustrated by the many control mandates found in compliance directives for finance, telecommunications, and cloud providers worldwide. Building new identity perimeters and restricting privileges to IT resources are musts. The transformed IT space demands new ways to control access to internal and cloud-hosted applications, the internet, and even in between applications. A framework that promotes the consistent authentication and authorization of an organization's privileged accounts can ensure security.

Securing Privileged Access in the Cloud

Africa has been a center of digitalization for the last few years and has seen rampant public cloud adoption. According to IDC's July 2023 Worldwide Software and Public Cloud Services Spending Guide, South Africa's public cloud services spending for will expand at a CAGR of 25.3% during 2021–2026. The rest of Sub-Saharan Africa (SSA) is seeing a similar adoption trend.

South Africa's public cloud services spending will expand at a CAGR of **25.3%** over the 2021–2026 period.

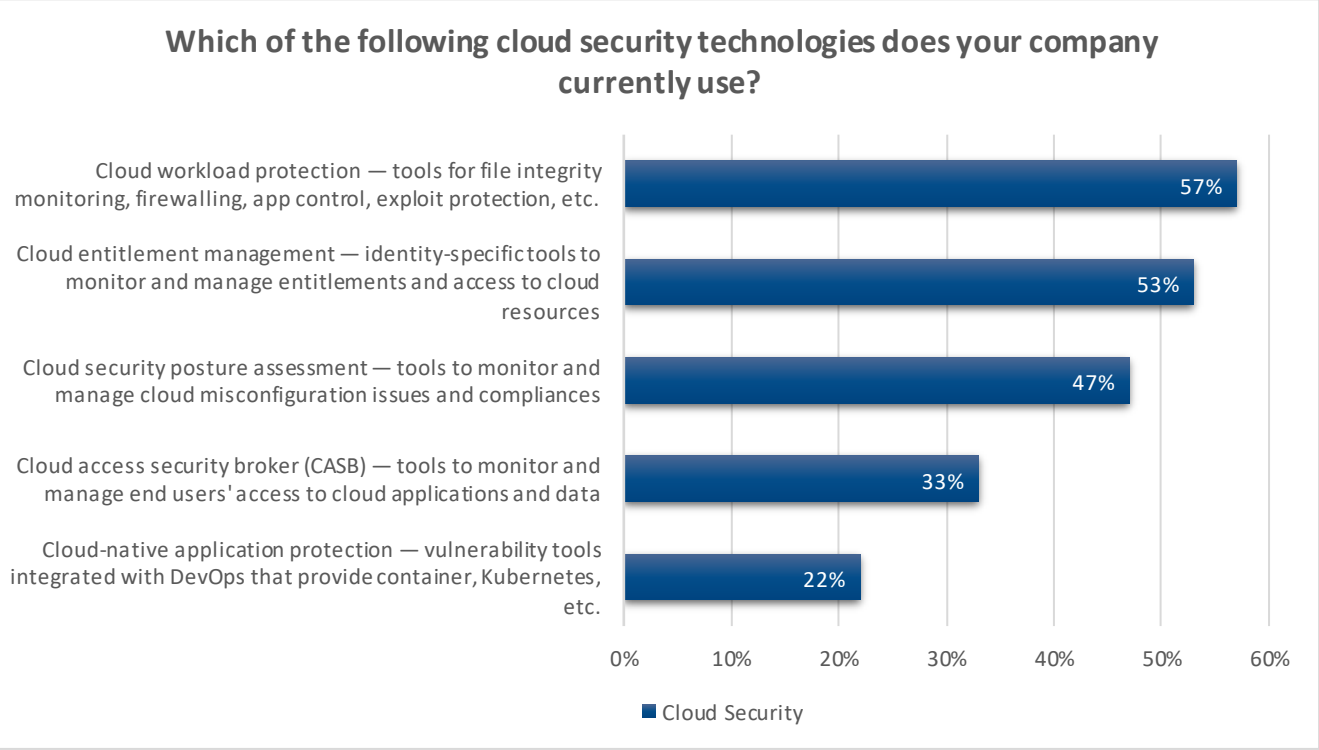
An observer might assume this cloud investment has been coupled with an equally enthusiastic cloud security investment. However, many organizations fall for a false sense of security in the cloud, ignoring the need for security ownership and accountability. This is a common occurrence not just in Africa, but across the world. Without the right monitoring and visibility, organizations risk losing control of user activities in the cloud. It is essential to understand that on-premises identity and access controls do not extend to cloud environments. Additional cloud-centric access solutions provide the required visibility and control.

As security awareness rises in Africa, organizations are focusing more on managing cloud entitlements, granular monitoring, and automated identity provision in clouds. Offered mostly as SaaS solutions, cloud identity and entitlement management (CIEM) has identity governance capabilities that help organizations manage privileges at scale by automating access requests, assignments, reviews, and expirations.

CIEM solutions enable organizations to grant, resolve, and revoke access entitlements for data, devices, and services — typically, using a least-privileged access methodology. These solutions improve visibility, detecting and remediating provisioning misconfigurations for both human and machine identities in multicloud environments. For admin users, the least-privileged principle should be implemented for all cloud access. This enables the possibility of full control over all authorized users who need to securely access cloud infrastructure. Just-in-time dynamic authentication is a key step toward achieving zero trust and effective user monitoring.

In IDC's *Security Survey, 2022* (September), 53% of respondents in South Africa regarded cloud entitlement management — or identity-specific tools to monitor/manage entitlements and access to cloud resources — as their second most important cloud investment priority for the following 12–18 months.

Figure 1: Cloud Security Investment Trends in South Africa

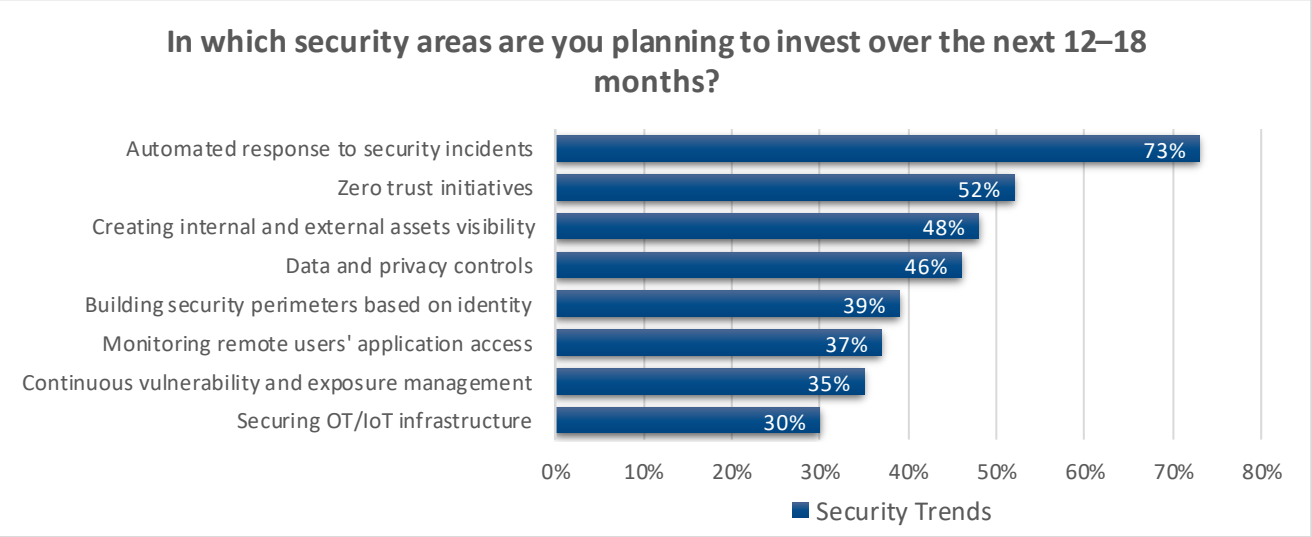


Source: IDC *Security Survey, 2022* (September); n = 51

Zero trust in Focus

The last two years have seen an increased focus on zero trust by CISOs in SSA. In an IDC *Security Survey* in January 2023, respondents in SSA ranked zero trust initiatives second in terms of expected investment over the next 12–18 months.

Figure 2: SSA Security Trends



Source: IDC *Security Survey, 2023* (January); SSA — n = 182

Organizations must understand that, at its core, zero trust focuses on building access controls based on identity and context. Zero trust emphasizes identity verification, authentication, and authorization — not just of users, but also of systems and devices. As such, identity and access mark the beginning of any zero trust project. A strong identity and access strategy is thus necessary for any zero trust initiative.

To begin their zero trust journeys, organizations must obtain robust mechanisms to verify identity and privileges and implement strong authentication. Privileged accounts should be at the center of these initiatives. Organizations should also implement a fine-grained least-privileged approach to access policy decisions. To achieve zero trust, users must be continuously verified. This is why zero trust principles point to adaptive trust.

IDC's recommendations resonate with CISOs in Africa. According to IDC's *Security Survey, 2022*, privileged access management (PAM) and identity and access management (IAM) were key projects on the zero trust journeys of 61% of CISOs in South Africa.

Special Publication 800-207, from the U.S. National Institute of Standards and Technology (NIST), offers an excellent starting guide for developing a zero trust strategy and road map. From a privileged access perspective, NIST recommends organizations focus on:

- Strong authentication that leverages user behavior analytics and uses a risk-based access policy
- Continuous verification to ensure that, at any given point of time, the right user has the right access to the right resources
- Privilege management that grants dynamic access to enterprise resources
- Monitoring access to detect behavior anomalies and drifts

Identity verification should make use of multiple attributes (e.g., geolocation, time, and role) to strengthen trust in an identity. After the identity of the user or system is verified, authorization mechanisms should kick in. It is important to monitor and record the activities of privileged accounts using authorized logins and to personalize

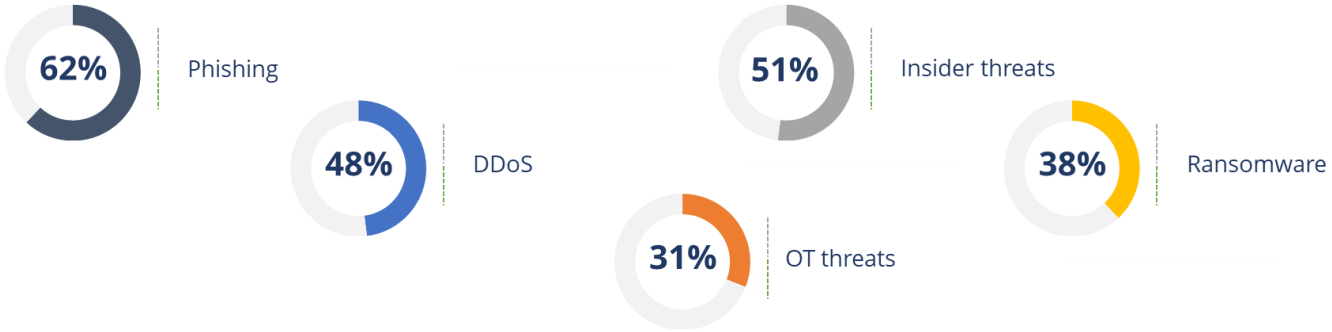
and manage access to sensitive data by granting access on a need-to-know basis. Continuous monitoring is essential to establish trust dynamically — a foundational principle of zero trust.

To build adaptive trust, organizations must apply and verify a least-privileged principle to ensure privileged accounts work with the least information and permissions necessary. Different technologies are applied in this area to achieve the broader concept of zero trust, but organizations should start the zero trust journey by strengthening privileged account security.

Rising Threats in Africa

Phishing and insider threats are among the top 5 threats in SSA. Indeed, IDC's *Security Survey, 2023* (January) found that phishing is the top threat in SSA.

Figure 3: Top 5 Threats in SSA in 2023



Source: IDC *Security Survey, 2023* (January); SSA — n = 182

The rate at which phishing is growing in the region is worrisome. With the increasing adoption of generative AI (GenAI) by hackers, cyberthreats — in particular, phishing — are likely to become even more severe. Threat actors can utilize GenAI to exploit human error, a key security vulnerability. They can use AI to exploit employees through social engineering, leveraging manipulations to commit security breaches or code errors. The use of AI can be expected to increase the frequency of sophisticated spear phishing attacks in which individuals and/or organizations are targeted with well-written, convincing, and personalized phishing emails.

Organizations are preparing for looming threats. We observe African organizations focusing on phishing security awareness campaigns and simulations. It is always recommended to have layered defense polices and tools to close gaps. Increased employee awareness is a positive trend — but, like any other learning, it has its own curve and adoption rates.

It is unreasonable for organizations to expect employees to scrutinize, with complete accuracy, all emails and attachments for potential phishing or fraud. The increasing use of AI in phishing suggests that even education will not be enough to defeat all threat actors. As a result, building strong authentication and privileged access controls — where all user access is tracked and monitored in real time — is imperative. Organizations must be prepared to enforce strong application, password management, and least-privileged controls to prevent phishing-initiated breaches. Preparation for a breach should always be the main plan.

Insiders are considered as users with some of the highest privileges within an organization and damages can be vast if no access perimeter is strictly defined. It's not surprising in these post COVID-19 times with increased remote and hybrid working arrangements using VPNs and remote desktop protocols, that insider threats scored the second highest of the top five threats. However, when we acknowledge that these remote access pathways are routinely exploited for vulnerabilities by threat actors, assessing the risk for any type of user to be given inbound access to internal applications when connecting remotely (not just admin accounts) becomes essential To prevent these risks, it is imperative that all internal users with privileges are duly monitored and managed, but without harming productivity so workers can still perform their daily operations. Access should be delivered on a specific who, when, where and what for basis. Organizations should be able to have live control on what is performed on systems and to report on any activity that was operated at any point of time.

Let's also focus on ransomware, which has been an increasing concern for cybersecurity teams. On a broad level, ransomware is an identity, privilege, and data access problem. To gain access to sensitive data, a threat actor first compromises an identity. If the right access policies are not enforced, the malware then moves laterally, with elevated privileges, across the infrastructure. To counter ransomware, it is essential that organizations mature their privileged access security measures and tie them to strong data security strategies and least-privileged policies. This is why PAM is also a sound defense against the threat of ransomware. The right access — with behavior monitoring — for admin users and machines is crucial. Identity nets around machines and workloads are an important yet often neglected area that can help restrict the lateral propagation of malware and reduce the blast surface.

Establishing digital trust is essential. Organizations should use public key infrastructure (PKI) digital certificates to provide validation that the user or machine is trusted and secure. Such identities function as the baseline for digital identities. Advanced controls include privileged access control, IAM, and identity-based segmentation.

It is essential that organizations enforce least privilege across all remote access sessions and apply just-in-time access policies for all remote admin sessions. Most compliance mandates require all privileged access sessions to be monitored and managed and evidence to be maintained.

Strategy to Secure Privileged Access

Current Privileged Access Maturity

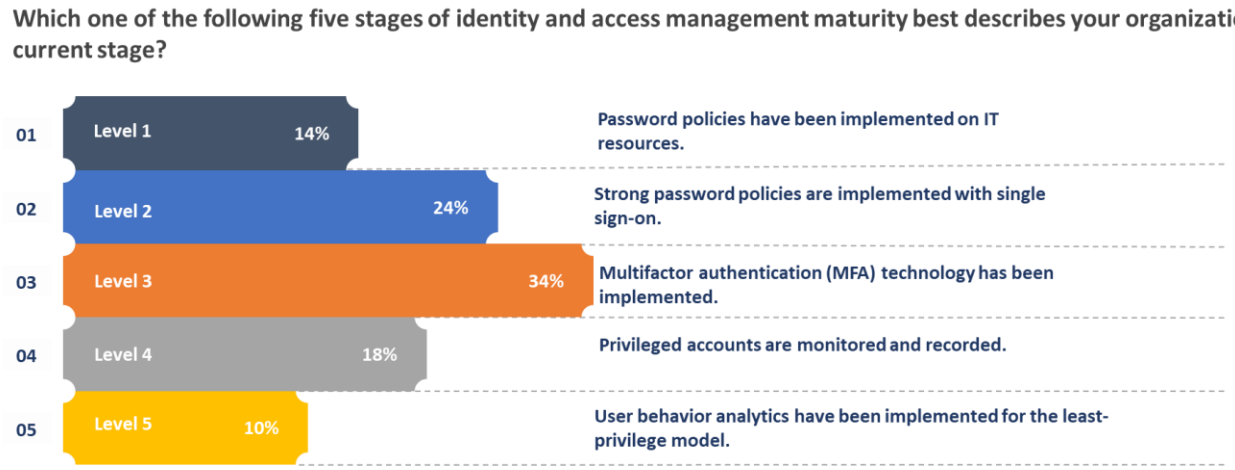
As stated earlier, investments in identity security in Africa have been low, despite the high rate of curated spear phishing attacks plaguing the continent. In early 2022, when IDC surveyed 209 organizations across SSA, just 18% said they were using PAM solutions.

Overall privileged access control adoption was indeed surprisingly low, but it was additionally worrisome that 25% of the 209 organizations were from the finance industry. In IDC's view, organizations in this highly regulated industry should ideally utilize a PAM solution for hygiene control 100% of the time.

Multifactor authentication (MFA) adoption stood at a mere 34% in September 2022, according to IDC survey data. Its predecessor, two-factor authentication, has been in the industry in various forms for 20+ years and should be seen as required for any organization determined to improve cybersecurity.

IDC regards these figures as unsettling, especially in a region that touts itself as being dedicated to establishing safer digital avenues for citizens and businesses alike and where organization across the board must protect the privacy of customers. More than ever, entities in Africa need to get serious about identity security.

Figure 4: Level of Privileged Access Maturity in SSA



Source: IDC *Security Survey, 2023* (January); SSA — n = 209

Some countries in SSA have issued security compliances that include privileged accounts:

- In 2018, the Central Bank of Nigeria issued its Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers. The directive includes guidance on managing and monitoring system administrators and privileged accounts.
- In its Joint Standard of 2022 Financial Sector Regulation Act draft, the South African Reserve Bank provided guidance on managing and monitoring privileged accounts.
- The 2018 Cyber & Information Security Directive from the Bank of Ghana set guidelines for securing privileged access to data, databases, and applications.
- The Central Bank of Kenya, in its 2018 Guidelines on Cybersecurity for Payment Service Providers, identified privileged access as a potential cyber-risk that must be monitored and controlled.

Road Map to Privileged Access Maturity

African organizations should no longer delay launching privileged access security initiatives — not only to counter cyberthreats, but because a privileged access control strategy creates business value by orchestrating and automating time-consuming manual tasks.

A phased approach should be adopted for any PAM project. Start by creating a business need for privileged access security in your organization. Once you have secured the budget, you can start selecting the right tools, functionalities, and frameworks for adoption. In tool selection, opt for a solution that:

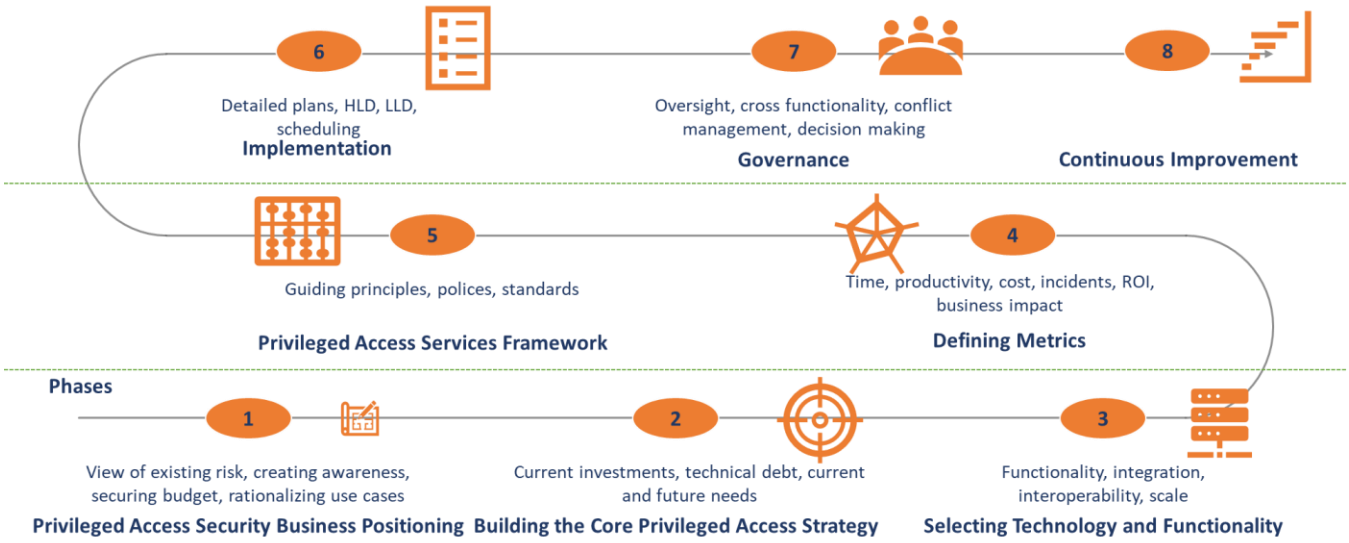
1. Provides complete coverage to automate passwords, manage sessions, audit user and administrator activity, and secure access for third-party and remote users

2. Provides an integrated platform with centralized management and reporting
3. Has product completeness in terms of features and enables integration with important third-party tools to create synergies (e.g., with identity threat detection and response [ITDR], a new category in identity security that focuses on collecting logs from different sources to enable real-time detection and response)
4. Features detailed reporting, including of metrics that helped you plan the business case to enable you to measure ROI

Next comes the implementation phase, where you will need to work at an operational level to manage potential roadblocks. Keep building upon your implementation plan to achieve success and your security and ROI goals.

The chart below spotlights the implementation phases IDC sees across organizations:

Figure 5: Phased Approach to Privileged Access Maturity



IDC Analyst Opinion

After a PAM implementation, organizations often debate how best to broaden their identity controls. What is eventually adopted usually depends on the use cases and complementary technologies already deployed by an organization. The market features a variety of products to address different strategies, but the most common include:

- IAM
- MFA
- Single sign-on
- Password management
- Digital signatures

In conclusion, PAM and identity form the core of modern security practices. Digital identities must be protected; these credentials are as vital as access itself. The importance of sound privileged access mechanisms cannot be

overstated. Breaches arising from privileged identity compromise can be financially crippling and even life-threatening. Securing digital and decentralized identities is the key to modernizing security approaches for cloud computing and SaaS adoption and to protecting organizations amid the dramatic shift to remote and hybrid business models.

Considering BeyondTrust

Protect Identities and Access from Cyberthreats with BeyondTrust

Identity is the new perimeter, and PAM is the keystone of modern identity and access security. No identities, human or machine, are more crucial to secure than those with privileged access to systems, data, applications, and other sensitive resources. PAM is essential in protecting your entire identity infrastructure, including your back-end IAM and identity governance and administration tools.

The expansion of remote work and cloud means organizations are grappling not just with more identities, but with more complex ones, as well. With privileged credentials and access in their possession, a cyberattacker or piece of malware essentially becomes an "insider." Threat actors are expanding their attack targets to include the very toolsets used to manage identities. This demands identity security for all accounts. Many breaches can still be prevented by simple security fundamentals, but attackers are rapidly advancing in agility beyond simple automation. Machine learning and AI are changing the game, vastly enhancing attackers' toolsets and empowering human-operated attacks.

GenAI is still in a nascent stage, but cyberattackers are already leveraging it to boost the speed, targeting, and sophistication of their workflows (e.g., by utilizing multi-step social engineering exploits to impersonate identities and their attributes). Almost every cyberattack today requires privilege for the initial exploit or to laterally move within a network. While the attack surface continues to expand and evolve, the most salient part of the story is how privileges continue to proliferate and become exposed in new ways. Identities are under attack from more angles than ever, and identity threats are hard to detect and increasingly complex. But complexity need not mean compromise.

BeyondTrust is the only identity security platform that allows you to detect threats across your entire identity estate and respond by controlling privileges, access, credentials, and other sensitive data.

With seamless integrations, unmatched discovery, and an identity-first data lake, we enable a zero trust approach to least privilege and intelligent threat detection to continuously strengthen your identity security posture.

BeyondTrust's PAM products empower you to protect identities, stop threats, and deliver dynamic access to enable and secure a work-from-anywhere world.

- **Password Safe:** Gain visibility and control of privileged credentials and secrets.
- **Privileged Remote Access:** Manage and audit employee and vendor remote access.
- **Remote Support:** Securely access and support any device or system in the world.

- **Active Directory Bridge:** Extend and manage Unix/Linux authentication and group policies.
- **Privileged Management for Unix and Linux:** Implement unmatched privileged access security.
- **Privileged Management for Windows and Mac:** Enforce least-privileged and control applications.
- **Identity Security Insights:** Gain a centralized view of identities, accounts, entitlements, and privileged access across your IT estate. Detect threats resulting from compromised identities and privileged access misuse.

BeyondTrust is a worldwide leader in intelligent identity and access security, enabling organizations to protect identities, stop threats, and deliver dynamic access. We are leading the charge in innovating identity-first security and are trusted by 20,000 customers, including 75 of the Fortune 100, plus a global ecosystem of partners. Learn more at www.beyondtrust.com.

About the Analyst

Shilpi Handa, Associate Director Research — Cybersecurity, IDC

Shilpi Handa is an associate research director at IDC, with responsibility for the Middle East, Turkey, and Africa cybersecurity practice. Her core research coverage revolves around cybersecurity, with a focus on network security, cloud security, application security, and security operations.