CYBERARK®
The Identity Security Company™

90 Identity Security Best Practices

This best practices guide gathers people, process, and controls considerations to maximize the efficiency and risk reduction of identity security programs. Find these three key categories below - with 30 recommendations each. **People** recommendations focus on staffing, people strategy, and reporting. **Process** recommendations to improve identity security program efficiency with an emphasis on automation, technology integrations, and defense-in-depth controls. **Controls** recommendations maximize risk reduction for identity-centric attacks.

	People	Learn More
01	Train all members of the workforce not to save work passwords and credentials for use on their personal laptops.	WHITEPAPER
02	Engage engineers developers to build champions for secrets management capabilities, facilitating adoption and scaling risk reduction.	SUCCESS BLOG
03	Build a staffing plan for your Identity Security program - complete with roles and responsibilities.	SUCCESS BLOG
04	Align IT, security, engineering and business stakeholders on Service Level Agreements and other key requirements for your Identity Security program.	SUCCESS BLOG
05	Customize the portal, tenant url and authentication templates of your Identity Provider to improve familiarity for employees.	SUCCESS BLOG
06	Build and re-asses an organizational change management plan when rolling out new Identity Secucity solutions.	SUCCESS BLOG
07	Define 'on-call' roles, responsibilities and processes for your Identity Security program to ensure operational resilience.	BLOG
08	Use gamification tactics like contests to promote end user adoption of new Identity Security controls.	SUCCESS BLOG

09	Build a RACI model (responsible, accountable, consulted, informed) for workforce access with single sign-on.	SUCCESS BLOG
10	Develop an Identity Security Awareness Kit when rolling out new technologies, to prepare end users for your.	BLOG
11	Educate the full workforce on risks and warning signs for common threats like social engineering, phishing and MFA fatigue attacks.	PODCAST
12	Educate employees on data handling and sharing policies.	BLOG
13	Encourage an 'assume breach' mindset for teammates across IT, security, risk & compliance.	BLOG
14	Develop safe reporting methods to ensure employees reporting insider threat concerns remain anonymous and protected from potential retaliation.	BLOG
15	Assign clear Security Operations Center (SOC) ownership for analyzing insider threat information and activity.	BLOG
16	Revisit employee cybersecurity training to ensure relevance in the age of generative AI.	BLOG
17	Communicate carefully with all employees about processes governing use of generative AI for proprietary data and information.	BLOG
18	Build a PAM business case for IT and security leadership - with clear KPIs.	WEBINAR
19	Create a training kit for new Identity Security program staffers to accelerate onboarding of new employees.	SUCCESS BLOG
20	Choose a clear, consistent and concise Safe Naming Convention for your PAM Program - and be sure to document it for scalability and long-term success.	SUCCESS BLOG
21	Identify security champions in your development organization to assist with the roll-out of Secrets Management capabilities.	SUCCESS BLOG
22	Equip developer champions for secrets management solutions with an 'objection handling' guide to overcome common questions from fellow engineers.	SUCCESS BLOG

23	Take a phased approach to securing vendor and third-party access to your environment, minimizing service disruptions while achieving program objectives on schedule.	SUCCESS BLOG
24	Design an effective reporting framework and 'score card' for your PAM program - and communicate the value to key business stakeholders.	BLOG
25	Build a roadmap for your Identity Security program - and continuously re-assess it with key Security, Risk and Compliance stakeholders.	SUCCESS BLOG
26	Develop and constantly re-assess KPIs for your PAM Program - with custom, consistent reports for IT & security leadership.	EBOOK
27	Educate company leadership - inside and outside of IT - to adopt a Zero Trust mindest.	WHITEPAPER
28	Align your cybersecurity goals to your company's mission, define key milestones in support of it and report on key metrics to inform business leaders from your program manager all the way up to the Board of Directors.	SUCCESS BLOG
29	Adapt process improvement frameworks like CMMI into your identity security program to assist in improving efficiency and maturity over time.	SUCCESS BLOG
30	Understand the difference between breadth and depth in identity security program maturity and maximize your capabilities to have the greatest impact.	SUCCESS BLOG

	Process	Learn More
31	Implement identity threat detection & response capabilities to detect and terminate anomalous usage of privileged accounts.	WHITEPAPER
32	Leverage automation and APIs to securely onboard privileged accounts at inception.	SUCCESS BLOG
33	Regularly test and update incident response playbooks and breach disclosure practices for identity-centric attacks.	WEBINAR
34	Automate the suspension and retirement of inactive accounts.	WEBINAR
35	When unable to eliminate passwords entirely, enforce strong and complex password policies for more secure credentials.	BLOG
36	Disallow SMS as a multi-factor authentication method, to reduce the risk of SIM Swap attacks.	BLOG
37	Integrate identity analytics (ITDR) capabilities with SIEM solutions. Bidirectional integrations strengthen threat detection and response.	INTEGRATION GUIDE
38	Limit user privileges based on the principle of least privilege - starting on the endpoint.	WEBINAR
39	Run disaster recovery exercises for any self-hosted privileged access management and identity security solutions.	SUCCESS BLOG
40	Standardize audit and compliance reporting across on-premises IT, SaaS and Iaas environments.	EXECUTIVE POV
41	Automate Identity Lifecycle Management tasks to reduce admin burden for Identity And Access Management Teams.	VIDEO
42	Wherever possible, enforce multiple layers of defense-in-depth controls to reduce risk.	WHITEPAPER
43	Implement a centralized logging system for all high-risk access - across privileged sessions	WHITEPAPER
44	Automatically review and govern access to enterprise systems on a continual and risk-based schedule	EBOOK
45	Implement account lockout policies and defense-in-depth protection to thwart brute-force password attacks.	BLOG

46	Regularly review and update access control lists to the most sensitive assets and services in your environment.	SUCCESS BLOG
47	Assess adoption of key privileged access management controls with telemetry data.	SUCCESS BLOG
48	Battle-test your Identity Security infrastructure with Red Team and Penetration Test exercises.	BLOG
49	Leverage low-code and no-code development engines in Identity Security solutions to automate identity lifecycle management tasks and security response actions.	SUCCESS BLOG
50	Reduce read-only permissions to cloud-hosted databases - even in dev, test and staging - to protect against data exfiltration.	BLOG
51	Secure application secrets used in identity security automation scripts.	SUCCESS BLOG
52	Develop an application inventory (CMDB) for all your enterprise deployed web apps and integrate it with your IDP to consistently secure all workforce access to web apps.	SUCCESS BLOG
53	Securely manage, rotate and restrict access to Root and Registration accouunts for your IaaS environments, in alignment with Cloud Service Provider recommendations.	SUCCESS BLOG
54	Leverage authentication assurance levels (AAL) when developing an MFA strategy for your organization.	EBOOK
55	Establish segregating duties (SoD) policies to require more than one person to complete the most sensitive operations, preventing error and privilege misuse.	BLOG
56	Continuously review all privileged accounts - and appropriately secure - both system and operational privileged access.	BLOG
57	Periodically review and assess your organization's security controls against the identity attack chain to identify gaps and vulnerabitlities.	SUCCESS BLOG
58	Prevent users from saving passwords in built-in browser password managers, reducing the number of accounts and credential repositories.	BLOG
59	Utilize risk-based priortization methodologies to influence your identity security focus, helping to rapidly mitigate the risk of identity takeover.	WHITEPAPER
60	Ensure users can only access critical hybrid and multi-cloud environments from trusted machines.	BLOG

	Controls	Learn More
61	Securely manage and rotate service accounts - a common 'back door' target for attackers - to the same standard as any Administrative account. For defense-in-depth protection, implement least privilege, adaptive MFA, session isolation and monitoring.	BLOG
62	Enable enterprise-grade password protection - for all personal employee passwords. Apply a higher standard of security to privileged admin, system and service accounts.	WHITEPAPER
63	Remove local admin rights on employee workstations - or, onboard them to a PAM solution. This can help prevent lateral movement and privilege escalation of ransomware.	EBOOK
64	Provide native user experience in privileged sessions for IT admins - whether they are accessing data center infrastructure, SaaS apps, elastic cloud workloads or cloud native services.	BLOG
65	In high-risk sessions to web apps, protect employee browsers from cookie hijacking attacks and prevent risky actions like downloading sensitive data	EBOOK
66	Securely store and manage authentication credentials - whether used by workforce users, IT admins, developers or non-human identities like service accounts.	WEBINAR
67	Use honeypots on employee workstations to improve identity threat detection and response capabilities, or detect and analyze potential ransomware threats.	BLOG
68	Eliminate secret zero and security island challenges with centralized secrets management.	DEVELOPER BLOG
69	Implement multi-factor authentication (MFA) for all users. Leverage biometrics and adaptive, context-aware MFA to implement a defense-in-depth approach.	VIDEO
70	Implement application control on employee workstations to protect against ransomware. If software can't execute, it can't deploy ransomware.	BLOG

71	Consistently secure and rotate credentials for domain accounts, local admin accounts, service accounts and application secrets.	WEBINAR
72	Apply extra security to third-party vendors with privileged access, such as just-in-time elevation, session isolation and audit.	WEBINAR
73	Continuously discover and onboard new devices and accounts when added to your network - including IoT devices - to securely manage and rotate credentials.	WHITEPAPER
74	Apply controls in-line with the risk of a user's access, to achieve a proper Zero Trust strategy.	SUCCESS BLOG
75	Securely manage, rotate and restrict access to Root and Registration accounts for your IaaS environments, in alignment with Cloud Service Provider recommendations.	BLOG
76	Protect your workforce with phishing-proof MFA factors such as number-matching authentication.	EBOOK
77	Kubernetes security best practices: Leverage native Kubernetes attributes to authenticate access to secrets and securely distribute secrets to k8s applications via mutual TLS SPIFFE-compliant x509 certificates.	DEVELOPER BLOG
78	Correlate all session risk-scores, audit logs, and session video playback, enabling auditors and forensics teams to skip to the moment of high-risk activity.	EBOOK
79	Protect high-risk workforce access to SaaS apps with precise session time limits and controls preventing sensitive actions (i.e. downloading sensitive data)	EBOOK
80	Enable secure vaulting and management of privileged account credentials used by software robots and RPA administrators.	EBOOK
81	Establish and monitor every identity, user and machine, behavior baseline to detect any abnormal behavior patterns.	WHITEPAPER
82	Think like the attacker and implement identity security controls that mitigate the core attack chain steps - prevent credential theft, stop lateral and vertical movement and limit privilege escalation and abuse.	SUCCESS BLOG

83	Don't let efficiency be your downfall - protect the scripts and tools your admins and operators use to accelerate their work with strong identity security controls.	SUCCESS BLOG
84	Proper cloud security requires a holistic approach to securing identities, mitigating risk at every access layer and resource within the cloud provider.	WHITEPAPER
85	Pursue a Zero Standing Privileges (ZSP) approach for operational access in cloud environments, to reduce credential theft and limit lateral movement.	BLOG
86	Secure software supply chains, pipeline artifacts and applications by Removing hardcoded secrets from CI/CD configuration files, scripts and code.	DEVELOPER BLOG
87	Simplify onboarding of third-party vendors to your PAM program with APIs, QR code invitations, and self-service workflows - eliminating the need for directory provisioning.	SUCCESS BLOG
88	Leverage a consistent solution to discover and secure local admin accounts across windows, mac and linux workstations and servers.	BLOG
89	Secure Robotic Process Automation (RPA) bot credentials with automated discovery, onboarding and rotation.	WHITEPAPER
90	Secure applications and service accounts in your cloud environments with a combination of secrets management, least privilege access, and lifecycle management controls.	SUCCESS BLOG