SECURE YOUR ENTERPRISE WITH THE POWERS OF IDENTITY AND PRIVILEGE

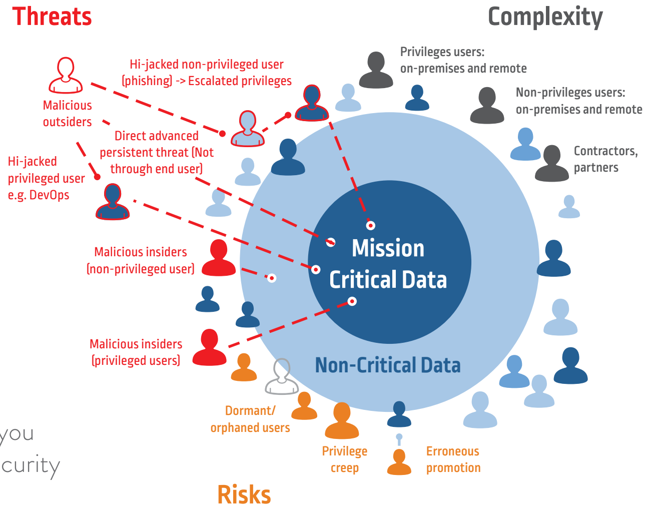
A CHECKLIST FOR EVALUATING YOUR CONTROL OVER WHO HAS ACCESS TO WHAT

In an ideal world, you'd know about and be able to manage the identity of every user (and application) with access to your systems and data, whether they are located on-premises and/or in the cloud.

In reality, you face the risks and complexities of managing a growing volume of different types of users—employees, contractors, partners—and cyber threats designed to exploit their identities and access rights.

Forrester estimates 80% of security breaches involve privileged credentials.[1] In a 2018 survey, 75% of respondents reuse passwords across different accounts, and 47% duplicate passwords across work and personal accounts.[2]

Interested in doing a quick check on where you stand in managing your non-privileged and privileged users/applications? This checklist is designed to help you identify where to focus your efforts to more effectively and efficiently close security gaps, reduce risk, and manage identity and access management.


Threats
Complexity
Hi-jacked non-privileged user (phishing) -> Escalated privileges
Privileges users: on-premises and remote
Malicious outsiders
Non-privileges users: on-premises and remote
Direct advanced persistent threat (Not through end user)
Hi-jacked privileged user e.g. DevOps
Contractors, partners
Mission Critical Data
Malicious insiders (non-privileged user)
Malicious insiders (privileged users)
Non-Critical Data
Dormant/ orphaned users
Privilege creep
Erroneous promotion
Risks

Do you have full visibility into each identity and system in your organization?	Need to do better	We're good	How well are you managing privileged account access of users and applications?	Need to do better	We're good	Are there any gaps in your management across non-privileged and privileged accounts?	Need to do better	We're good
	✓	✓		✓	✓		✓	✓
To what degree can you see who has access to what across your enterprise?			Do you feel in control of all privileged credentials across your entire IT infrastructure (including passwords, SSH keys, tokens, secrets, etc.)?			Do you have visibility across both non-privileged and privileged accounts from one vantage point?		
Do users complain about not having the right access to resources they need to do their jobs?			How well can you contain attacks on endpoints with the least privilege enforcement?			Can you run certifications, audits and reports that include both non-privileged and privileged accounts?		
How quickly can you validate user access requests against established policies?			Are you leveraging analytics to detect and alert on real-time, high-risk activity in privileged accounts?			Are there more cases of privileged access having been incorrectly or over assigned?		

[1] The Forrester Wave ™: Privileged Identity Management, Q4 2018

[2] SailPoint Market Pulse Survey 2018.

Do you have full visibility into each identity and system in your organization?	Need to do better	We're good	How well are you managing privileged account access of users and applications?	Need to do better	We're good	Are there any gaps in your management across non-privileged and privileged accounts?	Need to do better	We're good
	✓	✓		✓	✓		✓	✓
How hard is it to enforce compliance (e.g., segregation of duty (SoD), access certifications and audit reporting, etc.)?			To what degree are you able to provide credential protection for both users and applications (including COTS), whether they are on-premise or in the cloud?			Are you worried about hidden, unprotected credentials in your environment - such as dormant or orphaned, backdoor or service privileged accounts?		
How much effort does it take to ensure access is within corporate policy at all times?			Can you perform live monitoring and recording of user activity during privileged sessions?			Is the administration of credentials dispersed across different locations cumbersome and time-consuming?		
How much time do you spend creating, modifying and revoking access across the user lifecycle?			Can you isolate privileged sessions, especially those originating from outside the network and from unmanaged, third-party devices?			Do you find there has or could be a gradual creep of individuals' access rights beyond what they need to do their job?		
How fast can users change or reset passwords in the face of policies enforced across applications?			How tightly do you manage secured secrets used in DevOps environments?			Are you concerned that the lack of a unified access policy across all accounts is creating inconsistent access?		

Where Are You Most Vulnerable?

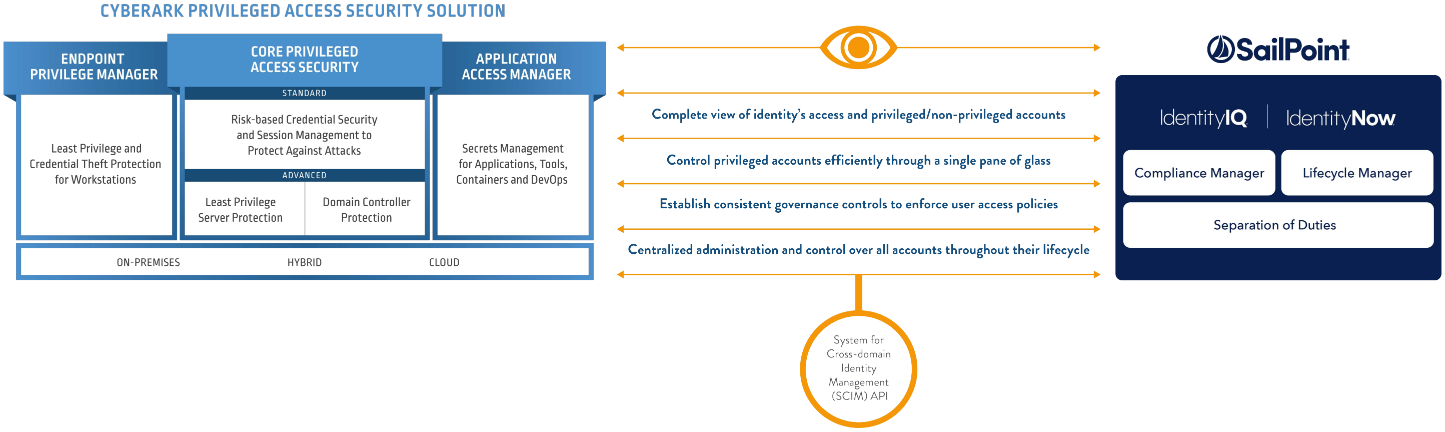
If you have several "need to do better" checkmarks in the first column, your company needs to implement stronger visibility and control through an identity governance solution. If your need for improvement falls in the middle of the chart, look to a privileged access security solution to safeguard your most critical assets and systems. Finally, if you are finding gaps between identity governance and privileged access security, as shown in the last column, choose a solution that more tightly integrates them. SailPoint and CyberArk solutions help you secure your enterprise with the powers of integrated identity and privilege.

Solution to Improve Your Visibility, Protect Privileged Access and Close Management Gaps

🟦 **SailPoint** Identity before governance solution provides complete visibility into who has access to what across the enterprise, empowers your users so they have the right access to the right resources to do their job, and enforces compliance with prevention and detection controls to ensure access is within corporate policy at all times.

🟩 **CyberArk Privileged Access Security Solution** provides the critical layer in privilege security that both strengthens and reinforces an organization's Identity and Access Management deployment. The solution delivers multi-layered protection from the inside out, from on-premises all the way into the cloud.

🟧 **CyberArk Privileged Access Security integrated with SailPoint** provides a unified, single pane of glass view with automated centralized policy-based identity governance for all identities, including privileged identities (individuals and applications) and access entitlements across the enterprise.


CYBERARK PRIVILEGED ACCESS SECURITY SOLUTION
ENDPOINT PRIVILEGE MANAGER
Least Privilege and Credential Theft Protection for Workstations
CORE PRIVILEGED ACCESS SECURITY
STANDARD
Risk-based Credential Security and Session Management to Protect Against Attacks
ADVANCED
Least Privilege Server Protection
Domain Controller Protection
APPLICATION ACCESS MANAGER
Secrets Management for Applications, Tools, Containers and DevOps
ON-PREMISES
HYBRID
CLOUD
Complete view of identity's access and privileged/non-privileged accounts
Control privileged accounts efficiently through a single pane of glass
Establish consistent governance controls to enforce user access policies
Centralized administration and control over all accounts throughout their lifecycle
System for Cross-domain Identity Management (SCIM) API
SailPoint
IdentityIQ
IdentityNow
Compliance Manager
Lifecycle Manager
Separation of Duties

To learn how to address improvements in areas identified in the checklist, contact your sales representative or visit us at www.sailpoint.com or www.cyberark.com

About CyberArk

CyberArk is the global leader in privileged access security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. To learn more, visit www.cyberark.com.

SailPoint: The Power of Identity™

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies in a wide range of industries, including: 6 of the top 15 banks, 4 of the top 6 healthcare insurance and managed care providers, 8 of the top 15 property and casualty insurance providers, 5 of the top 15 pharmaceutical companies, and six of the largest 15 federal agencies. To learn more, visit www.sailpoint.com.

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.