Adoption framework for Zero Standing Privilege

Supporting runtime access control for production access

The Cyber Hut

Contents

Executive summary

Runtime access control introduces the ability for organizations to deliver improved capabilities for discovering, securing and monitoring privileged access and accounts. The capabilities, benefits and integration options vary from more traditional PAM solutions that were often on-premises. This modern approach supports a "Zero Standing Privilege" way for developers, engineers and security staff to have a decoupled way of accessing core high risk resources. Risk reduces, productivity increases and access becomes more consistently applied.

Adoption drivers

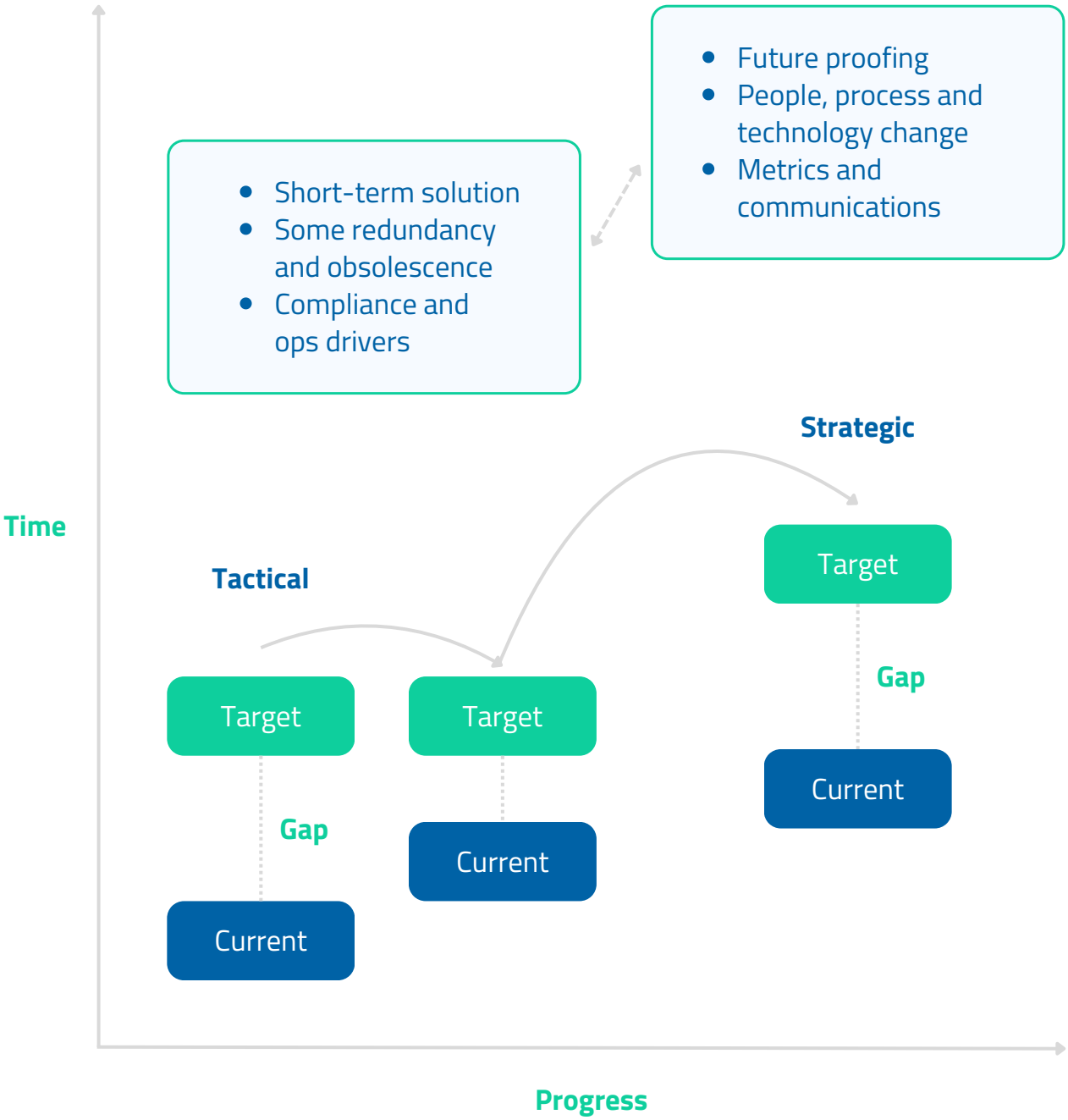
- **Identity-centric attacks**: they are on the rise, from both internal and external adversarial behaviour. The likelihood and impact of such attacks has risen due to the strategic evolution of identity and access management (IAM) in general.

- **Compliance**: Regulated industries have to contend with who has access and who is accessing key critical assets—yet this is becoming more complex due to a broader array of assets under protection as well as varying degrees of protocols and integration avenues

- **Hybrid deployment**: more assets, more identities and a broader attack surface is complicated by many organizations having to support on-premises, private cloud, cloud service provider (CSP) and SaaS resources—amplifying a need for a consistent management and control plane that improves developer and engineering productivity by decoupling access and risk

This adoption framework document provides security and operations leaders with a set of steps that allow them to understand their current position with respect to the management of high-risk assets and infrastructure access, requirements and maturity, and in turn develop internal business case and roadmap artifacts to trigger adoption of Zero Standing Privilege platforms.

Adoption progress



Adoption progress

Current profile—Where you are

Business objectives discovery

People, process and technology

Location of high-risk systems

Ownership of high-risk systems

Risk appetite understanding

Governance and access process model

Business objectives discovery

Access flows into systems

Protocols into high risk systems

Identities and account in use

Authentification modals in use

Permissions being used

Vulnerability analysis and threat model

Target profile—Where to go

What can't be done today?

Business—Deliver products and services rapidly, agile response to change, engineering productivity

Security—Consistent MFA, Just in time access, E2E visibility, broad coverage of systems integrated

What could be done tomorrow?

Business—Technology transformation, informed risk analysis, faster service delivery, dev/eng productivity increase

Security—Central control plane for all high risk access, consistent application of controls

Adoption progress

Current profile assessment

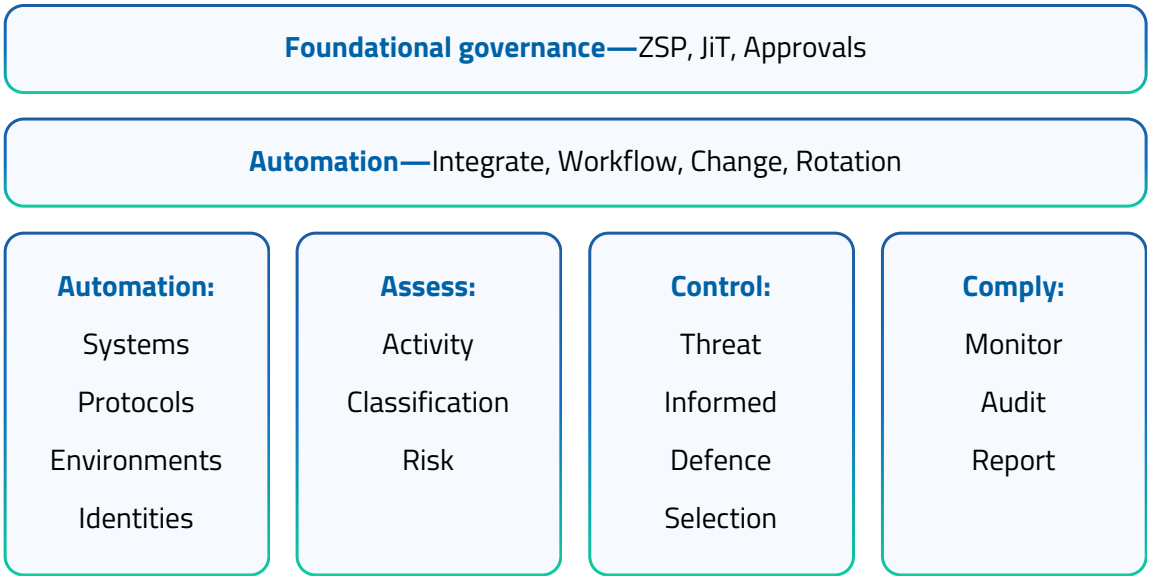
#	Assessment point	Details
CPA-1	Understand existing privileged infrastructure landscape	Tools, environments, integrated systems, protocols, access locations
CPA-2	Understand existing privileged asset landscape	Identities, repositories, policies, permissions, approval mechanisms
CPA-3	Understand stakeholder involvement	Teams, titles, job involved in requesting, approving and accessing privileged resources
CPA-4	How are privileged identities authenticated?	Security versus usability audit. MFA coverage. Consolidation opportunities
CPA-5	How are privileged identities authorized?	Access request processes. Policy design. Policy enforcement. Access review. JiT/ZSP maturity.
CPA-6	How are credentials management?	Issuance, rotation, revocation flows and processes.
CPA-7	Which systems are not in scope?	Why? Integration and management challenges.
CPA-8	How is the current privileged model integrating to business objectives?	Help point. Hinder points. Metrics and communications.

Adoption progress

Target profile design

#	Design point	Details
TPD-1	Which existing systems are not under management?	Their roadmap, longevity, risk. Limiting factors
TPD-2	Which future systems are planned?	Integration requirements, locations, protocols, owners
TPD-3	Which protocols are not under management today?	Their roadmap, longevity, risk. Limiting factors
TPD-4	Which environments will be leveraged in 3 years?	On-premises, hybrid, PaaS, CSP
TPD-5	What authentication modals will be leveraged in 3 years?	Passwordless. MFA. Consolidation.

Framework



Foundational governance

The adoption journey is grounded in foundational governance principles. Firstly the strategic migration to a zero standing privilege (ZSP) model where no identity or account has pre-provisioned permissions or credentials when not in use. This reduces the identity attack surface, improves security controls assurance and focuses monitoring on high risk usage. The implementation of ZSP relies upon the ability to deliver Just in Time (JiT) access request and fulfillment management. Permissions and credentials are associated with live identities and accounts at the correct time of event processing—which has been verified, validated and approved. All systems and access flows should leverage these three principles over time.

Automation

Central to a strategic identity-first model, is the ability to integrate more identities, more systems and from more locations. To achieve this, automation is essential. No-code orchestration provides a non-technical and cross-stakeholder approach to broadening the coverage of the privileged access management system, likely via an API-first integration approach. The onboarding and management of protected systems and repositories of interest should not be limited by integration and connectivity challenges. Protocols, locations and interfaces coverage should be broad and expandable. Change of workflow and rotation of associated credentials and permissions is expected.

Framework

Automation

An understanding of the existing and future landscape of systems, identities and accounts should be automated, allowing for changes to protocols and integrated repositories. Discovery mechanisms should be an immediate step in business or infrastructure change.

Assess

Informed risk management requires an assessment of the vulnerabilities, impact and likelihood of threats against the target privileged access management base. Privileged access data and runtime behaviours should be classified with appropriate alerting and triage.

Control

Selection of controls such as authentication, credential rotation, permissions change, monitoring and so on, should be defined via a threat informed defensive model that can strategically support the ability to handle “unknown unknown” patterns of adversarial behaviour.

Comply

The creation of a secure running state for privileged access should be consistently maintained in line with the business risk appetite and compliance needs and the external threat landscape.

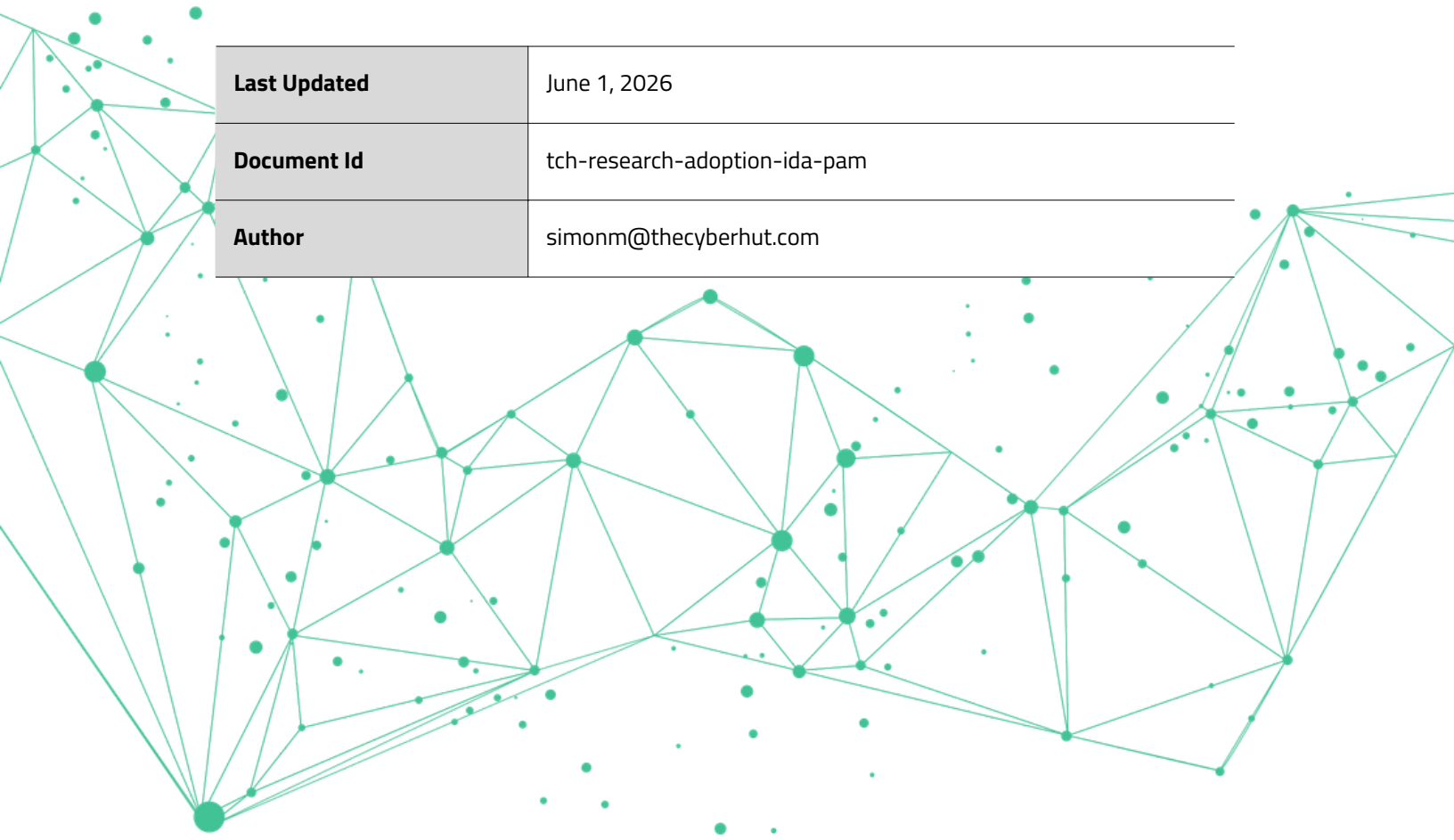
Disclaimer

The Cyber Hut opinion in this document represents the view at the time of writing. Recommendations, comment and opinion is subject to change as market conditions and product maturity alters. The Cyber Hut does not provide legal or financial advice. The Cyber Hut shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

The Cyber Hut provides impartial and neutral commentary on technology within the identity and security communities—helping buyers and investors understand the complexities with respect to technology, concepts and market patterns.

The Cyber Hut was founded in 2021 to provide a range of training, advisory, market analysis and research services covering the emerging technologies within the identity and security industries.

For further information, please contact **info@thecyberhut.com**



Last Updated	June 1, 2026
Document Id	tch-research-adoption-ida-pam
Author	simonm@thecyberhut.com

P0 SECURITY

Contact Us

Email: info@p0.dev
Web: www.p0.dev

P0P0 Security is the central AuthZ Control Plane™ for agents and users, helping enterprises secure runtime access for the modern workforce. P0 governs the full action chain across agents and users, enforcing least-privilege policy with real-time context, so organizations can control what agents do and with whose authority before they take action in sensitive systems.

Built on a foundation of Zero Standing Privilege and runtime policy enforcement, P0 replaces broad permissions and static credentials with just-enough privilege, just-in-time access and fully traceability activity – avoiding the access control failures that expose enterprise data and critical systems.

Zero Standing Privilege. Zero added friction. Because secure runtime access is Priority Zero™.

Learn more at www.p0.dev.