

		PHASES OF MATURITY			
		PHASE 0: HIGH RISK 0	PHASE 1: FOUNDATIONAL 1 Get visibility & reduce attack surface	PHASE 2: ENHANCED 2 Integrate policies & limit overprivileged users	PHASE 3: ADAPTIVE 3 Increase automation & intelligence
DIMENSIONS OF MATURITY	<p>GRC</p> <p>Governance, Risk and Compliance</p> <ul style="list-style-type: none"> • AU - Audit & Accountability • CM - Config Management • RA, SA - Risk & Security Assessment • SI - System & Info Integrity 	<ul style="list-style-type: none"> → No PAM Vault → No centralized inventory of all assets in the environment. → No easy way to report on user access permissions and privileges. 	<ul style="list-style-type: none"> → Establish an accurate inventory of privileged accounts and passwords. → Classify credentials and secrets. 	<ul style="list-style-type: none"> → Discover, classify, and manage local accounts, groups, roles, and security configuration files that might grant privileges across all assets. → Implement real-time session monitoring and security access control policies for endpoints. → Enforce host-based session, file, and process auditing with integration to SIEM. Integration with → ITSM for change control approvals. 	<ul style="list-style-type: none"> → Integration with IGA for attestation reporting and risk-based approvals. → Leverage audit data, machine learning analytics, and automation to detect, track and alert to any threats (Integrate with EUBA). → Discover and classify service accounts. Implement service account discovery, provisioning, and governance across identity and cloud service providers. → Harden operating systems and app components.
	<p>PA</p> <p>Privileged Administration</p> <ul style="list-style-type: none"> • Specific controls from • AC - Access Control • CM - Configuration Management • MA - Maintenance • SC - System & Communications Protection SP 	<ul style="list-style-type: none"> → Users may be admins of their own workstations. → Workstation security cannot be trusted. → May be managing administration for Windows Servers using Domain Admin group membership. → May be managing local accounts on each UNIX/Linux system and may be editing the local SUDO file. 	<ul style="list-style-type: none"> → Vault and automate periodic rotation for all administration accounts. → Vault Active Directory and Azure privileged accounts and manage privileged groups. → Discover and vault local admin accounts. → Establish a secure admin environment for both local and remote sessions. → Establish initial privileged access workflows. 	<ul style="list-style-type: none"> → Establish basic privilege elevation policies for all endpoints (Workstations and Servers). → Establish just-in-time, just-enough privileges (JIT & JEP). → Discover and vault Linux and local admin credentials (passwords and SSH keys). → Expand remote access control to vendors and contractors without creating AD accounts. 	<ul style="list-style-type: none"> → Establish more granular policies for privilege elevation. → Automate onboarding of new managed assets.
	<p>IAM</p> <p>Identity and Access Management</p> <ul style="list-style-type: none"> • AC - Access Control • IA - Identity & Authentication 	<ul style="list-style-type: none"> → No centralized access controls. → Admins access using local admin accounts. → Near impossible to tell who has access and what privileges they have. → Identity management may not be centralized. 	<ul style="list-style-type: none"> → Enforce MFA for access to Vault, including secrets check out and remote session initiation. → Establish alternative admin accounts to prevent using public identities. → Enforce alternative admin and MFA for remote access. 	<ul style="list-style-type: none"> → Enforce Multi-Factor Authentication at endpoints for direct log-in and privilege elevation → Eliminate local accounts via identity consolidation for UNIX and Linux Servers. → Remove hardcoded credentials and config data from applications and scripts. → Automate privilege security in DevOps workflows and tooling. 	<ul style="list-style-type: none"> → Ensure all connections required for privileged operations must be mutually authenticated with cryptographic credentials. → Increase MFA from NIST Authenticator Assurance Level 1 (authenticating with an ID and password) to NIST Authenticator Assurance Level 2 (AAL2). AAL2 has more identity assurance due to the presence of a second factor. → Restrict privileged access to only registered and company-owned endpoints. → Prohibit privileged access by any client system that is not known, authenticated, properly secured, and trusted. → Require dual authorization for privileged operations on critical or sensitive systems.
	<p>Products & Process</p>		<ul style="list-style-type: none"> → Products <ul style="list-style-type: none"> • PAM Vault - Secret Server • Bastion Service - Remote Access Service • Connection Manager (optional) → Integrations <ul style="list-style-type: none"> • SIEM → Process Changes <ul style="list-style-type: none"> • PAM Vault Training • Remote Access Training 	<ul style="list-style-type: none"> → Products <ul style="list-style-type: none"> • Server PAM - Server & Cloud Suite • Workstation PAM - Privilege Manager • DevOps Secrets Vault → Integrations <ul style="list-style-type: none"> • ITSM for change control, trouble tickets • SIEM → Process Changes <ul style="list-style-type: none"> • Privilege Elevation training • Help Desk support process changes • Third-party access training 	<ul style="list-style-type: none"> → Products <ul style="list-style-type: none"> • Privilege Behavior Analytics • Account Lifecycle Manager → Integrations <ul style="list-style-type: none"> • IGA • SIEM & EUBA → Process Changes <ul style="list-style-type: none"> • App Developer Security Training • Automate security and compliance

Aligning with security and privacy controls as defined in NIST 800-53 (<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>)