ManageEngine
PAM360

Get cyber insurance ready with ManageEngine PAM360

The one-stop PAM checklist for all your cyber insurance needs

Cyber insurance protects the interests of organizations in the event of cyber incidents related to their IT network infrastructure and security.

In the past 3 years, cyber insurance payouts have increased by a hefty 200%, with the peak number of claims adding up to 8,100 in 2021 alone. Though the amount of claims might seem exorbitant, a market study suggests that only 55% of all organizations have cyber insurance policies in place at all.

This has consequentially led to cyber insurance policies becoming more stringent with high premium costs and mandated vigilance over the security of all IT entities.

Cyber insurance providers recognize privilege access management (PAM) controls as pivotal to an organization's security posture. Such controls play a foundational role in impeding diverse cyber threats and curtailing the ramifications of a data breach.

In this brochure, we will explore how a PAM solution can help you meet such intricate cyber insurance requirements. We'll specifically focus on how PAM360 implements critical PAM ideologies that will optimize your next cyber insurance purchase, to ensure you'll be deemed eligible for minimized premium costs and larger insurance claims.

Cyber insurance requirements	Recommended best practices	How PAM360 helps
Does your organization have any measures in place to manage privileged identities?	Discover, group, regulate, and share all privileged identities across the organization's IT network securely.	PAM360 can discover, consolidate, and onboard users and endpoints from an array of enterprise directory services into the solution. It then assigns specific roles and responsibilities to such privileged users and endpoints respectively, and groups them according to the requirements demanded by the organization’s access policy. Using PAM360, you can selectively and securely share such privileged accounts in remote endpoints to privileged users.
Do all employees of your organization use multi-factor authentication (MFA) while logging in to their enterprise IT assets and software?	Authenticate users logging in to the solution with credentials stored in the respective directory, and enforce MFA for all users of the IT asset or software.	PAM360 offers a wide range of integrations with all enterprise-wide MFA solutions such as Google Authenticator, Microsoft Authenticator, Okta Verify, RSA SecurID, YubiKey, to name a few. PAM360 also comes with a native TOTP app, Zoho OneAuth, that supports biometrics-based user authentication.

Cyber insurance requirements	Recommended best practices	How PAM360 helps
What steps do your organization take to prevent, detect, and deter ransomware attacks?	Prevent malware manipulation by implementing regulated access to endpoints, enforce the four-eyes principle for endpoint access requests, standardize least privilege practice, and enforce stringent network segmentation.	PAM360 enables selective sharing of privileged accounts in remote endpoints to individual users or a group of users by verifying user roles and responsibilities. PAM360 enables sharing of such privileged information through password request-release workflows. These access requests are first raised by the user with a mentioned purpose, then are granted approval by a selected admin. Administrators can set up temporary, monitored, just-in-time (JIT) access to highly privileged resources through native privilege elevation and delegation management (PEDM) controls that can terminate the session in the event of suspicious activity. Using PAM360's policy based access control (PBAC) module, **admins can create** customizable access policies based on user and device trust-scores and other vital factors. Trust-scores are derived dynamically based on various security parameters such as network legitimacy, user and endpoint behavior, and more. For every privilege that is anointed to a user, our solution places a fail-safe that monitors, prevents, detects, and deters such privileges from being misused.

Cyber insurance requirements	Recommended best practices	How PAM360 helps
Does your organization keep track of all privileged activity in the network?	Audit and register all privileged activity regarding who, when, and where a privileged session was initiated, and record what activities were performed during such privileged sessions. The "what" may include, but is not limited to, password changes, access requests approved and denied, remote sessions, and users and resources onboarded and offboarded.	PAM360's audits and reports are a comprehensive archive of all activity performed by all users of the solution. The audits and reports widely range from endpoint and user activity reports and privileged sessions (active and recorded) reports to SSH keys and SSL/TLS certificate operations reports. Additionally, PAM360 provides users with the ability to generate reports using structural query language (SQL). The complete schema of the PAM360 database is available for the database administrators to leverage, based on which, users can regulate report generation with database queries to achieve SOX and HIPPA requirements. PAM360 enables enterprises to record all privileged activity performed via the solution, which security teams use for audits and forensic purposes.
Do all your employees have admin access?	Segregate administrative access for privileged users and grant least privilege access for other users.	PAM360 works on the principle of least privilege. Every control, by default, is functionally displaced to provide the least privilege required for a specific user. This functionality is completely customizable and lets organizations deploy unique user roles to enforce role-based access control.

Cyber insurance requirements	Recommended best practices	How PAM360 helps
		All features and functionalities are fine-tuned coherently to reflect the principle of least privilege across the enterprise, thus limiting admin access to selective users who need it, when they need it.
Does your organization have controls in place to assist in backup and recovery in the event of a cyber incident?	Back up critical data, deploy emergency measures, and ensure quick data restoration based on predefined criteria.	PAM360's break-glass configuration helps users back up all privileged identities and ensures automatic enabling of fail-safe mechanisms based on admin-selected criteria. PAM360's failover services are fully automated to operate in adverse situations; they don't require manual intervention. Inevitably, if the unforeseen does occur, use PAM360's read-only backup server to provide uninterrupted access to all your critical data. These break-glass and offline access capabilities are also accessible remotely through mobile applications for both Android and iOS handheld devices. Note that such features and back-up procedures are only accessible by users with high privileges, thus avoiding unauthorized enablement of emergency measures.

Cyber insurance requirements	Recommended best practices	How PAM360 helps
Are your organizational IT solutions compliant with the latest software standards?	Address critical IT requirements such as governmental guidelines or recognized IT standards, while acknowledging established recommendations by the data protection regulations.	PAM360 offers out-of-the-box report generation for government and industry regulations such as PCI DSS, ISO/IEC 27001, NERC CIP, and the GDPR. These reports can be obtained clause-wise or entirely depending on the requirement. The PAM solution scans your endpoints to validate if they are in compliance or in violation the respective standard. In the case of a violation, PAM360 will suggest remediation steps.
How does your organization prevent unnoticed expiration of website certificates and network device keys?	Create, secure, deploy, and manage SSL/TLS certificates for websites, other endpoints, and network SSH keys.	PAM360's native certificate and key management module offers end-to-end life-cycle management of SSL/TLS certificates and SSH keys through extensive integrations with third-party certificate authorities such as GoDaddy, Verisign, DigiCert, Thawte, and more. PAM360 also alerts admins before expiry of such critical certificates and keys, thus empowering them with complete governance and management of certificates and keys. This significantly reduces the administrative overhead that naturally arises while managing certificates and keys manually. PAM360 eliminates the need for a stand-alone IT solution to manage SSH keys and SSL/TLS certificates.

The above listed questions are derived from critical cyber-insurance requirements that insurers use to test the eligibility of their prospect for lower premium rates and higher insurance claims.

To summarize, organizations are expected to implement:

- Multi-factor authentication
- Statutory measures against cyberattacks
- Centrally accessible secret vaulting
- Monitored secret sharing
- Regulated certification of IT assets
- Software that facilitates the achievement of compliance standards
- Reliable back-up mechanisms
- Mandated audit trails of all privileged activity

Optimize your cyber insurance process with PAM360

ManageEngine PAM360 is the flagship product of ManageEngine's privileged access management suite. PAM360 is well recognized by industry analysts for its flexible deployment options, ease of use and maintenance, and quick-use features that are designed to reduce operational fatigue and prioritize security over everything else.

PAM360 is fine-tuned and regularly audited to meet yearly cyber insurance requirements and is up-to-date with 2023 insurance metrics. With that said, over 5,000 customers from all over the globe trust ManageEngine's PAM suite to meet their cyber insurance eligibility requirements for reduced insurance premiums and increased payouts.

Reduce your cyberattack surface and effectively meet your cyber insurance needs with PAM360

Talk to our experts

Start a free trial