



# Meet Cyber Insurance Requirements with PAM

---

Whitepaper



## Index

1. Introduction.....	03
2. Securing Cyber Insurance Becomes a Necessity.....	03
3. Cyber Insurance Underwriters & Their Evaluation Criteria.....	04
5. Securden Helps Comply With Major Security Requirements..	05
6. Automate Security Best Practices With Unified PAM.....	06

## Introduction: Digital Transformation Creates New Attack Venues



Digital transformation is paving the way for several organizations to operate better and deliver value to customers. Cloud adoption, and hybrid environments have become common among startups as well as enterprise organizations.

With the growth in technology, there are equally persistent threats – malicious actors are finding new vulnerabilities among emerging tech stacks used by organizations and exploit them to their advantage.

Cybercriminals leverage these new attack venues to breach sensitive data and put a hold on critical operations - turning organizations into marionettes and holding them under ransom until they give in to demands. While monetary demands themselves would cause an organization heavy loss, stoppage of critical systems could present a bigger issue. Service providers, government agencies, and other service industries have multiple other businesses/people dependent on them who may get directly affected

### **Weak foundations topple even the most secure organizations**

---

The lack of following basic security practices is found to be the reason for exploitation, time and again. While malicious attackers target and breach even the most complex networks, their tactics boil down to executing the most basic attack strategies including phishing, credential compromise, ransomware and exploitation through malicious insiders.

## Securing Cyber Insurance Becomes a Necessity



Incurring a huge loss from paying ransom or costs from recovering critical systems may cause organizations to shut down their business. The long tail costs of a data breach can

extend for months to years and include significant expenses that companies are not aware of or do not anticipate in their planning. To tackle these colossal costs, organizations look to secure a cyber-insurance plan that will help them recover financially in the event of a cyberattack.

Cyber insurance, being a relatively new arm of the insurance industry, has found difficulty in defining intricate policies due to a lack of understanding of the risks involved. This is largely due to the continuously evolving nature of cyberattacks. Recently, AI has also had an effect on how cyberinsurance underwriters write their policies.

They have thus decided to give organizations cyber-insurance based on a set of mandatory, basic security controls. And for certain cases, they have added exclusions and exceptions such as breach due to fault of a third-party or the organization not reporting immediately to the cyber-insurance company.

## **Ransomware Causes Cyber-insurers to Raise the Bar**

Insurers are seeking robust security measures that they believe can effectively prevent, detect, and respond to malicious activities throughout the ransomware lifecycle. While cyber insurers pose a wide array of questions in their applications, certain key themes have emerged that reflect their primary concerns about ransomware and the security controls they view as most effective in addressing those concerns. Insurance companies require insureds to fill in a supplemental application that is used for the evaluation of a submission for insurance. Coverage is now conditional - granted based on how far the company is aligned with the expected controls.

## **Cyber Insurance Underwriters and Their Evaluation Criteria**

Cyber Insurance underwriters carefully review catastrophic incidents and create cybersecurity practices for organizations to follow. Insurers require organizations to fill out the 'Ransomware Supplemental Application' with checkboxes on common security practices.

## **Security controls that keep organizations secure in 2024**

Following a set of security best practices largely limits the attack surface. These measures not only qualify the organization for larger insurance coverage – it ultimately reduces the risk of falling prey to a cyberattack.

These security measures, on a high level can be divided into the following 10 categories:

- Employee Awareness and Security Training
- Identity, Access and Credential Security
- Endpoint Detection & Response
- Vulnerability Management Controls
- Multifactor Authentication on all Privileged Accounts
- Vendor and Third-party Access Controls
- Secure RDP/VPN Access
- Internet Defense and Email Security
- Data Backups and Disaster Recovery
- Comprehensive Auditing and Reporting

## **Following Safety Requirements Mandatory**

While organizations may manage to secure cyber insurance, if they fail to keep in line with the safety measures recommended by the policy – the claim for insurance will be denied by the company. This requires continuous compliance with best practices and therefore its automation.

**Securden Unified PAM helps comply with major security requirements**



While organizations often require a handful of solutions to cover basic practices, Securden Unified PAM encompasses major security controls without the need for a segmented approach.

The areas that Securden Unified PAM covers include (but not limited to) are:

- Endpoint and Server Security – Application Control
- Data Security – Credential and Secrets Vaulting
- MFA to privileged accounts / resources / logins
- Internal / External Access Controls
- Vendor / Third-party Access Management
- VPN-less Secure Remote Access (RDP / SSH / SQL)
- Local admin accounts, service accounts and dependencies management
- On-demand privilege elevation, Just-in-time access, Approval workflows, and LAPS are some of the other supplemental functionalities.

## Automate Security Best Practices With Securden Unified PAM




Securden Unified PAM is built for modern organizations with on-prem / cloud / hybrid environments to provide holistic access security without the need for multiple products or a complex deployment.


The mapping below has been prepared by studying various ransomware supplemental applications that organizations are required to submit for obtaining a cyberinsurance. The table presents the category of each requirement followed by how Securden Unified PAM helps satisfy them.


Specific Controls that Cyber-insurers require		How Securden Unified PAM helps
Security Control Category <b>1. User Access Controls</b>		
1.	Prevention of unauthorized access to critical endpoints and systems.	Through control policies, Securden unified PAM grants access to critical IT resources such as servers, systems and network devices through multiple levels of authentication. This ensures that only authorized personnel can access critical IT assets.


Specific Controls that Cyber-insurers require		 <b>How Securden Unified PAM helps</b>
<b>Security Control Category</b> <b>1. User Access Controls</b>		
2.	User access rights reviewed annually, at a minimum.	Through comprehensive access logging and reporting capabilities, <b>Securden Unified PAM</b> lets administrators review user access rights at any point of time. Reports can be scheduled and automatically sent to auditors / admins who need to review user access rights.
3.	Users must be assigned access based on their job responsibilities and role.	Role-Based Access Controls can be defined in <b>Securden Unified PAM</b> to assign users access based on their job responsibility. Organizations can define custom roles for users with varying granular permissions.
4.	Monitoring of user/admin accounts for communication with malicious websites, IP addresses, and other threat group resources	All privileged accounts onboarded in <b>Securden Unified PAM</b> can be prevented from communicating with restricted IP addresses.
5.	Identification and elimination of access provisioned to inactive users.	<b>Securden Unified PAM</b> has a comprehensive auditing and reporting system which allows generating reports of inactive users and the access permissions they have. These permissions can be revoked based on the information collected from the report.
6.	Access granted to employees no longer in the organization must be revoked.	Users who leave the organization can be handled in multiple ways with Unified PAM. Since <b>Securden Unified PAM</b> integrates with your AD / Azure AD, users removed from AD will subsequently be removed from <b>Securden Unified PAM</b> . You can also manually transfer the accounts / passwords owned by the leaving employee and then either remove them from the solution or block their access to the <b>Securden Unified PAM</b> interface.
7.	Access control request workflows based on valid help desk tickets.	<b>Securden Unified PAM</b> integrates with ticketing systems so that users who need access to an account can be given access once one or more approvers authorize it, they can also mention the time duration of access by provisioning JIT privileges.


Specific Controls that Cyber-insurers require		 How Securden Unified PAM helps
Security Control Category <b>1. User Access Controls</b>		
8.	Ensure multiple levels of checks before allowing access to servers.	Securden Unified PAM lets you add your server accounts in the repository through discovery. Once added, multiple checks can be configured to access this server – by logging in with SSO, enforcing MFA, integrating with TOTP etc.
9.	Access to a system is authorized only if based upon Legitimate business need for access and the least amount of access needed to perform job duties (i.e., “Least Privilege” access).	Users who need access to a system can be enforced to provide a valid reason for their access, and once vetted by the administrator, Securden Unified PAM authorizes the access request. The authority who grants access can also choose to limit this access based on the user’s job responsibilities.
Security Control Category <b>2. Vendor and Third-Party Access Controls</b>		
1.	Documented management processes in place for the selection and oversight of third-party access	All third parties who require access to sensitive internal IT assets can be granted secure, monitored access through Securden Unified PAM.
2.	Third-party access controls in place to restrict “Always on” permission to corporate resources.	Securden Unified PAM allows provisioning vendors with time restricted, on-demand access to corporate systems and IT assets, this ensures that vendors cannot abuse their privileged access. All activity performed during access is captured in detailed audit logs to hold them accountable.
3.	External parties (vendors, subcontractors, etc.) have access only to systems and applicable data within scope	Securden Unified PAM helps limit the scope of access for vendors, contractors and third-party users who need to access internal systems. They would only be given the least privilege that is required to carry out their jobs.



Specific Controls that Cyber-insurers require		 How Securden Unified PAM helps
Security Control Category <b>3. Credential and Data Security Controls</b>		
1.	Passwords, SSH keys, and other secrets automatically rotated according to a defined schedule, or after each use	Securden Unified PAM defining a schedule by which passwords, SSH keys and other credentials can be automatically and periodically rotated – the complexity of rotated credentials can be defined using a password policy. Passwords can also be rotated after being used.
2.	Password management policies enforced across all privileged access points	Once all sensitive accounts and systems are added in Securden Unified PAM, it acts as the point of access for any user to utilize organizational data/systems. This point of access can
3.	Formally documented password policies dictating length, strength, history.	Securden Unified PAM has the facility to define granular password policies which can dictate various password attributes such as: Password length, history, strength, preventing use of specific characters/words, password age, characters to start with, etc.
4.	Dynamic calls / API calls in place to eliminate embedded or hard-coded credentials	Securden Unified PAM allows automation of any task that can be performed within the solution by means of RESTful APIs which are very comprehensive. This helps eliminate credentials that are hardcoded in scripts and applications.
5.	Secure collection and handling of customer data.	Companies that store customer data can ensure that this data is accessible to no other internal / external user. This in turn may help with GDPR compliance.
6.	Passwords and privileged user accounts are unique from each other.	Securden Unified PAM has a powerful password analysis engine which prevents users from using duplicate passwords and ensures that all credentials and user account passwords are unique from each other.

Specific Controls that Cyber-insurers require		 How Securden Unified PAM helps
Security Control Category <b>3. Credential and Data Security Controls</b>		
7.	Employee password risk awareness, solution to prevent users from using simple or breached passwords.	Securden Unified PAM has a dark-web monitoring feature that informs users if they are utilizing passwords that were part of a data breach, and also warns them if the passwords in use are non-compliant with the password complexities defined by the password policy.
Security Control Category <b>4. Privileged Accounts Security</b>		
1.	Privileged and service accounts must have lengthy passwords which are rotated periodically.	All privileged accounts, service accounts and dependencies associated with windows system accounts can have their passwords rotated periodically based on the policy defined within Securden Unified PAM.
2.	Domain admin accounts - Require MFA, must be managed and monitored through JIT access, require approval to provide privileged access.	Domain admin accounts added to Securden Unified PAM can be configured to allow access only upon successfully authentication by MFA. This access can be configured to be time-restricted and only be granted upon approval by an administrator.
3.	Inventory of all user accounts, admin accounts and authorisation of active accounts	All user accounts, admin accounts, service accounts and dependencies are stored securely in a central encrypted repository. This serves as the inventory of all privileged accounts in Securden Unified PAM, and authorization can be enforced through multiple ways.
4.	Count of all domain, privileged and service accounts.	Reports and dashboards in PAM can provide the count of all domain, privileged, and service accounts stored in the solution.

Specific Controls that Cyber-insurers require		 How Securden Unified PAM helps
Security Control Category <b>5. Endpoint and Malware Defense</b>		
5.	Application controls across workstations to only allow for execution of authorized applications. Unauthorized applications are blocked, and the list of authorized applications is reassessed at least bi-annually.	Privilege elevation and delegation controls in <b>Securden Unified PAM</b> allow defining centralized application control policies. This can allow execution of only the authorized/approved applications and block all unauthorized applications. The administrator can re-assess the authorized (allowlisted) applications by generating bi-annual reports and reassess if it needs any change.
6.	Tool to find unmanaged assets and list them at least weekly	<b>Securden Unified PAM</b> deploys agents on endpoints for privilege management, these can help provide an update of assets that may be unmanaged.
7.	Inventory of 'Vital Assets' and SIEM to collect their logs	Vital assets can be added in <b>Securden Unified PAM</b> through network discovery and then integrated with SIEM to collect syslogs generated when users access these assets through the <b>Securden Unified PAM</b> interface.
8.	Granular policies must be defined for privilege elevation.	Privilege elevation and delegation capabilities of <b>Securden Unified PAM</b> allow defining granular application control policies. These policies can be very comprehensive, allowing only specific users / user groups to access specific application(s) on specific computers/computer groups.
9.	Local admin rights removed for users on workstations / servers	<b>Securden Unified PAM</b> helps eliminate the local administrator rights across all workstations and server using the lightweight Securden agent installed on these endpoints.
Security Control Category <b>6. Remote Access and Privileged Session Security</b>		
1.	Remote Access - protected / restricted remote access to systems and networks containing customer data.	<b>Securden Unified PAM</b> supports remote access via SSH, SQL and RDP protocols to systems and IT assets in the network.

Specific Controls that Cyber-insurers require		 How Securden Unified PAM helps
Security Control Category <b>6. Remote Access and Privileged Session Security</b>		
2.	Troubleshooting and administration of remote of systems must be performed over secure channels.	For troubleshooting purposes, Securden Unified PAM has provisions to create technician access policies so that remote systems administration can be done over secure channels.
3.	All remote access must have a first layer of username-password auth followed by an MFA, vendor remote access must be managed.	Securden Unified PAM can be configured to enforce user authentication and then authenticate through MFA before they can launch connections to remote systems. Vendors and third-parties also go through this process to launch remote connections to sensitive assets.
4.	RDP connections to workstations must be protected.	All RDP connections launched from Securden Unified PAM to Windows workstations are encrypted and protected.
5.	Privileged account passwords are not revealed to the user when checked out, and access is recorded through a session management tool.	Securden Unified PAM ensures that remote connections to assets/systems can be launched without revealing the account credentials to the end user. Once the connection is terminated, the password can optionally be changed too. All connections launched are recorded with a session management tool and can be monitored live as well.
6.	Domain admin account logs must be captured, and access sessions must be recorded.	All activity carried out by users using domain accounts are logged comprehensively and their access sessions are recorded in detail, capturing both their keystrokes and video of the actions they perform.
Security Control Category <b>7. Auditing and reporting capabilities</b>		
1.	Systems are configured to issue a log entry and alert when an account is added to or removed from a domain administrators' group or when a new local administrator account is added on the system.	When critical events such as admin account addition or removal occur on endpoints, Securden Unified PAM can notify these events and also log these actions.

Specific Controls that Cyber-insurers require		 How Securden Unified PAM helps
Security Control Category <b>7. Auditing and reporting capabilities</b>		
2.	Logging and monitoring is in place for changes to existing user accounts (e.g., password reset, modification to access levels or groups, etc.)	Securden readily integrates with all SIEM solutions including SPLUNK, IBM QRadar, LogRhythm among others. Logs and activities can be sent in any format suitable for the preferred solution.
3.	Implement real-time session recording and security access control policies for server endpoints.	<p>Privilege session recording can be enforced on all accounts stored in Securden. Web-based and native sessions launched from Securden are recorded and the keystrokes are logged.</p> <p>It is also possible to enforce real-time session monitoring and recording for servers selectively.</p> <p>Securden provides an exhaustive list of tamper-proof reports that can be exported as and when required.</p>

**Securden Unified PAM** offers the essential capabilities to secure sensitive data and control access to critical resources, aligning with the requirements of cyber insurance policies. With comprehensive access controls, customizable reports, auditing features, and privileged management of endpoint systems and remote sessions, organizations can effectively mitigate risks.

These capabilities are adaptable for companies operating on-premises, in the cloud, or within hybrid environments, ensuring they meet the stringent security standards required for maintaining cyber insurance coverage.