BeyondTrust

Meet Insurance Requirements with PAM

Cybersecurity Insurance Checklist

The blistering pace and expanding scope of cyberthreats and ransomware attacks is forcing cyber insurance companies to steeply increase their rates and premiums, and even drop coverage for high-risk organizations. Underwriting requirements to be approved for cyber insurance are becoming more stringent.

BeyondTrust Privileged Access Management (PAM) solutions provide the foundational security that cyber insurers demand for reducing risk and liability, from external and internal cyber threat actors.

Our products enable essential capabilities, such as least privilege enforcement, privileged account and credential management, and remote access security, that are needed to qualify for cybersecurity insurance.

Cybersecurity Insurance Checklist

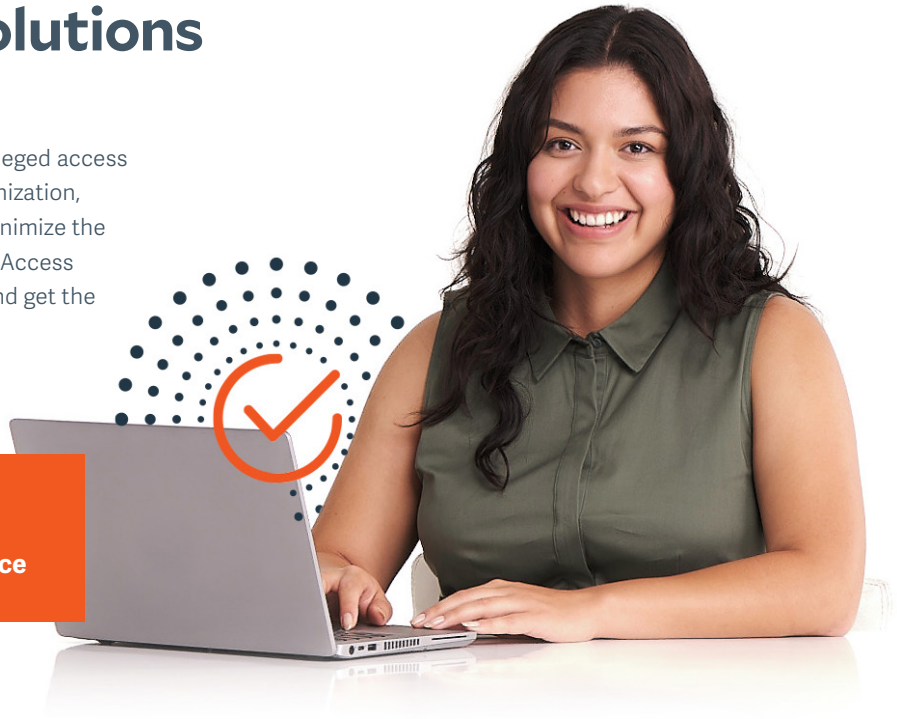
Common Eligibility Questions	How PAM Can Help	BeyondTrust Value
Do your users have local admin rights on their laptops or desktops?	Removes all admin rights and elevates access, as needed, to applications based on the proper content, and only for the duration needed.	Admin rights removal is one of the most powerful ways to reduce the attack surface and defend against both external and internal threats. **BeyondTrust protects your estate right away, allowing you to analyze behavior and refine policies as you go.** By removing admin rights and elevating applications, not users, you can achieve true least privilege on day one, without restricting productivity.
Can you confirm human and non-human accounts abide by least privilege at all times?	Enforces least privilege and application control across all human and non-human identities and accounts across any type of endpoint or other asset.	Least privilege enforcement significantly reduces the attack surface. It can help protect organizations against tricky, fileless threats and zero day exploits. **BeyondTrust solutions help you apply the principle of least privilege across your entire IT ecosystem, including human and non-human identities.** Our solutions help you right-size privileges and permissions on-premises and across your cloud infrastructure.
What protections are in place to protect remote access to the corporate network?	Proxies access to the corporate network, applications, assets, and makes all connections outbound—no VPN needed.	Management of all privileged remote sessions from vendors and employees, including vaulting credentials, ensures fine-grained access control—no matter where a session originates. **With BeyondTrust, all your connections can be brokered through a single access pathway, reducing the attack surface, while providing a single list of authorized endpoints available for each user.** End-user experience will also improve as all endpoints are accessed via a single interface.
Do you manage privileged accounts using tooling or software solutions?	Discovers, manages, controls, monitors, and audits all privileged account activity across your entire IT infrastructure.	PAM solutions are built for securing and managing all types of privileged accounts. **BeyondTrust solutions help you discover, secure, control, monitor, alert and record access to all privileged accounts.** With BeyondTrust, you can also leverage privileged threat analytics and reporting to address cyber insurance and compliance requirements.
Do you use multi-factor authentication for remote network access originating from outside your network by employees and third parties (e.g. VPN, remote desktop)?	Provides built-in multi-factor authentication for remote access, as well as the ability to seamlessly integrate with third-party MFA tools.	MFA provides an extra layer to ensure that access is only given to the right identity. **BeyondTrust provides native multi-factor authentication for remote access by employees and third parties, and also provides seamless integration with leading MFA solutions, enabling you to get the most of your technology investments.**

Cybersecurity Insurance Checklist

Common Eligibility Questions	How PAM Can Help	BeyondTrust Value
Do you utilize any unsupported operating systems or platforms? If so, what compensating controls are in place for these systems or platforms?	Restricts privileges to the minimum necessary to help limit any potential misuse of systems or platforms.	**BeyondTrust solutions help you apply the principle of least privilege for human and non-human users, mitigating potential misuse or compromise of any system.** Our solutions can also proxy access and enforce segmentation or microsegmentation to broadly isolate unsupported and risky platforms from other networked assets to help contain spread of potential breaches. Privileged credential rotation and session monitoring ensures that all privileged activity is controlled and monitored, safeguarding your critical assets.
Have you reviewed your environment for the Indicators of Compromise (IoC) to confirm that none were found?	Captures all privileged session data, including keystroke logs, screen recording, commands typed/executed, and more that can help pinpoint breaches and the internal pathways of threat actors.	**BeyondTrust solutions can help you gain a centralized view of all assets, accounts, and users in your environment. Information gathered is correlated with baselines for normal behavior, identifies changes, and alerts on anomalies that can signal the presence of critical threats.** Our solutions can also identify IoCs that suggest lateral movement or potentially inappropriate privilege escalation, either from commands or rogue user behavior, while file integrity monitoring illuminates any suspicious changes in Unix/Linux systems.
If Indicators of Compromise were found, have they been remediated?	Implements rotation of compromised credentials to stop access and prevent password re-use attacks. Privileged access rights can also be restricted or removed to further reduce ability for lateral movement and malware execution.	**BeyondTrust provides several mechanisms to prevent data compromise, as well as post-compromise remediation.** Our solutions enable alerting based on anomalous activity to help prevent misuse or theft of privileged credentials. Credential rotation can also be implemented to prevent attacks or immediately after a credential is compromised. User admin rights can also be restricted to mitigate any movement across the network or malware execution.
Describe any steps that you take to detect and prevent ransomware attacks.	Prevents and mitigates ransomware and malware from landing and expanding by implementing robust security over remote access, onboarding and managing privileged credentials, and enforcing least privilege and application control.	**BeyondTrust solutions provide comprehensive coverage of use cases associated with ransomware, malware, and other cyberthreats.** Our solutions can help you thwart any ransomware, malware, or human operator from achieving lateral movement and privilege escalation to advance an attack, keeping bad actors marooned at the initial point of compromise.

Qualify for Cybersecurity Insurance and Reduce Cyber Risk with BeyondTrust PAM Solutions

Cybersecurity insurance companies recognize that privileged access security controls are foundational security in every organization, prevent many cyberattacks outright, and significantly minimize the damage of any potential breach. BeyondTrust Privileged Access Management can help you qualify for cyber insurance and get the best rates, while drastically reducing your cyber risk.



Learn More
beyondtrust.com/solutions/cyber-insurance

BeyondTrust

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

beyondtrust.com