BeyondTrust

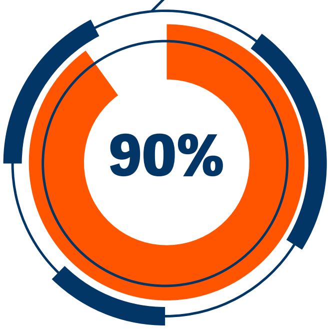
Cybersecurity Insurance Requirements Checklist

Meet Cyber Insurance Requirements with Identity Security & PAM

With AI powering new threats, and the growing surge of ransomware and identity-based attacks in recent years, the demand for cyber insurance coverage is only expected to increase.[1] At the same time, cyber insurers are continuously re-calibrating risk and policy underwriting requirements in response to the evolving threat landscape.

Cyber insurers have a vested financial interest in understanding risk, and they recognize how identities, their access, and their privileges are at the heart of damaging cyberattacks.

- **90% of organizations experienced at least one identity-related security incident over the past year[2].**
- **Ransomware is projected to cost victims $265 billion annually by 2031.[3]**



BeyondTrust solutions provide the foundational security that cyber insurers demand for reducing risk and liability, from external and internal cyber threat actors.

Below is a checklist of common security controls and capabilities cyber insurers will typically require to qualify for a policy. Also, learn how BeyondTrust privileged access management (PAM) and identity security capabilities address these requirements.

Common Eligibility Questions	The BeyondTrust Value
Do users have local admin rights on their laptops, desktops, or workstations?	BeyondTrust protects endpoints and identities by eliminating local admin rights. Elevate access for applications—not users—just for the finite moments needed, and for the proper context. Protect your estate from Day 1, with BeyondTrust endpoint privilege management capabilities, then analyze behavior and refine policies as you go. This implementation of least privilege not only sharply reduces the attack surface, but also defends against external and internal threats—all without hindering user productivity.

[1] Q2 2023 Market Segment Report. AM Best. June 2023.
[2] Trends in Securing Digital Identities Report. IDSA. June 2023.
[3] Who's Who in Ransomware Report. Cybersecurity Ventures. September 2023.

Common Eligibility Questions	The BeyondTrust Value
Can you confirm human and non-human accounts abide by the principle of least privilege at all times?	BeyondTrust enforces least privilege for human and non-human / machine identities across all endpoints (servers, desktops, IoT / OT, etc.), applications, and assets. Intelligent application control capabilities enforce granular access for applications, and also stop tricky fileless attacks by leveraging built-in, context-based security to catch bad scripts and infected attachments, and to control child processes and DLLs. BeyondTrust also provides centralized visibility and intelligence of identities and accounts across your entire multicloud and on-premises estate. This enables you to continuously right-size entitlements and maintain a least privilege posture, even for highly dynamic cloud environments.
What protections are in place to protect remote access to the corporate network?	BeyondTrust enables fine-grained access control and oversight no matter where a session begins or ends. Proxy access to the corporate network, infrastructure, applications, and other assets. Make all connections outbound—no VPN needed. Brokering remote connections via BeyondTrust through a single access pathway, while providing a single list of authorized endpoints available for each user, reduces the attack surface, while also improving end-user experience. Leverage robust, real-time session monitoring and management, with capabilities like recording, keystroke logging, and the ability to pause or terminate a suspicious in-progress session. Also benefit from continuous visibility into all remote access and identities across your environment, and the ability to swiftly address or mitigate potentially malicious activity. BeyondTrust further extends privileged access management and identity security best practices beyond the perimeter by layering on MFA, and vaulting and managing credentials, injecting them directly into sessions—never revealing them to an end user.

Common Eligibility Questions	The BeyondTrust Value
Do you use multi-factor authentication (MFA) for remote network access originating from outside your network by employees and third parties (e.g. VPN, remote desktop)?	BeyondTrust provides native multi-factor authentication for remote access by employees and third parties. Our PAM solutions also seamlessly integrate with leading MFA solutions for other use cases, enabling you to get the most of your technology investments, while further bolstering identity security. In addition, BeyondTrust can identify and alert on account misconfigurations (such as lack of MFA on a privileged account), so you can quickly remediate such instances and ensure optimal protection.
How are you managing third-party and/or vendor access?	BeyondTrust provides robust vendor privileged access management (VPAM) capabilities to extend security best practices to all third parties. This includes providing secure, VPN-less access, implementing least privilege, onboarding and managing vendor credentials, controlling and auditing sessions, and detecting and mitigating potential risks or attacks.
Do you manage privileged accounts using tooling or software solutions?	BeyondTrust is recognized as a privileged account management leader by all the top analysts. Our privileged access management (PAM) solutions discover, onboard, manage, control, monitor, and audit all privileged accounts and sessions across your entire IT infrastructure. Ensure proper security hygiene for privileged passwords, accounts, keys, secrets, business application passwords, and sessions for people and machines. This also includes service accounts, which are a type of non-human account that cyber insurance brokers are highly concerned about because they are often unmanaged and can be exploited to compromise systems and applications. With BeyondTrust, you can also leverage privileged threat analytics and holistic identity security visibility and reporting to ensure identities and accounts are properly secured and have the right amount of access and privileges, to further satisfy cyber insurance and compliance requirements.

Common Eligibility Questions	The BeyondTrust Value
Do you utilize any unsupported operating systems or platforms? If so, what compensating controls are in place for these systems or platforms?	BeyondTrust restricts privileges to only the minimum necessary, applying the principle of least privilege across your environment. This helps mitigate potential misuse or compromise of any system. Our solutions can also proxy access and apply a number of zero trust controls, including enforcing segmentation and microsegmentation, to isolate unsupported and risky platforms. This helps prevent the spread of potential breaches between segments. Additionally, BeyondTrust capabilities around privileged credential rotation, session monitoring, and holistic visibility of your identity estate, ensure controlled and monitored privileged activity, safeguarding critical assets.
Have you reviewed your environment for the Indicators of Compromise (IOCs) to confirm that none were found?	BeyondTrust provides groundbreaking visibility over enterprise identity security posture and threats. Our solutions also capture comprehensive privileged session data, including keystroke logs, screen recordings, and executed commands. Quickly pinpoint in-progress attacks on identities and internal threat pathways. Zero in on IOCs signaling lateral movement or inappropriate privilege escalation. In addition, file integrity monitoring highlights suspicious changes in Linux systems.
If Indicators of Compromise were found, have they been remediated?	BeyondTrust can rapidly identify and help remediate indicators of compromise and in-progress attacks. Just a few key ways BeyondTrust can remediate detected attacks include: • Implementing credential rotation to stop access and prevent password re-use attacks. • Eliminating, or further restricting, privileged access rights or cloud entitlements to reduce lateral movement and stop malware execution and spread. • Pausing sessions for review, or terminating them, to stop potentially dangerous activity.

Common Eligibility Questions	The BeyondTrust Value
Describe any steps that you take to detect and prevent ransomware attacks.	BeyondTrust provides powerful, blended threat protection that disrupts multiple steps of the ransomware attack chain, whether involving humans or malware. These cyber defenses include: • Robust remote access security controls • Onboarding and managing of privileged credentials • Continuous enforcement of least privilege and application control • Holistic identity threat visibility, detection, and response. BeyondTrust security capabilities prevent many ransomware threats from landing and executing, restrict attempts at lateral movement and privilege escalation, and also quickly identify and mitigate potential attack surfaces (such as excess privilege, orphaned accounts, lack of MFA, etc.) or in-progress attacks. Additionally, all BeyondTrust solutions comply with backup and recovery requirements of cyber insurance brokers. Such requirements include high availability, geographical disbursement, and data backup. In the aftermath of a ransomware attack, it's important to know with certainty that your data backups and recovery falls within cyber insurance policy compliance.

Next Steps:

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

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

Contact BeyondTrust today, or learn more here: beyondtrust.com/solutions/cyber-insurance