
CyberQP
OBTAIN
CYBER
INSURANCE
WITHOUT
THE HASSLE
How MSPs and IT Leaders Can Secure Coverage, Avoid Denials, and Prove Compliance with Confidence

TABLE OF CONTENTS

How to Use This Guide

Cyber insurance used to be simple. A quick form, a few yes-or-no questions, and a policy was issued. Not anymore.

Today's underwriters demand more than intentions. They require proof. That includes policies, audit logs, access control documentation, and verifiable implementation of technical safeguards such as multi-factor authentication (MFA), privileged access management (PAM), and identity governance.

If you're an MSP completing cyber insurance applications across multiple clients, or an internal IT/security leader working directly with carriers, you've likely already felt the shift. The controls haven't changed, but the burden of evidence has.

This guide will help you:

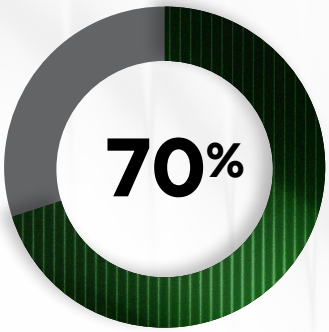
- Understand what cyber insurance carriers are really looking for
- Identify the most common control areas where applications fail
- Discover why traditional tools often fall short
- Learn how to prove compliance before an underwriter or incident response team asks

CyberQP helps IT professionals and service providers operationalize security controls in a way that aligns with real insurance requirements, so when you say "yes" on an application, you can back it up.

The State of the Cyber Insurance Market

Cyber insurance is no longer a light-touch safeguard. It's a high-stakes gatekeeper, and the stakes are rising.

According to the IBM Cost of a Data Breach Report 2025, the average breach cost surged to $4.45 million, a 15% increase over the past three years. As ransomware continues to devastate small and mid-sized businesses, carriers have responded by tightening eligibility, increasing scrutiny, and shifting risk back onto policyholders.



"70% of ransomware-related claims were denied in 2025 due to misrepresented or unprovable controls."

— SeedPod Cyber

The Beazley Cyber Insurance Application asks for clarity on:

- Data encryption methods
- Patch management frequency
- Incident response processes
- Security governance ownership

The CRC Group Short Form and CRES Cyber Liability Questionnaire go further, requesting:

- How MFA is enforced across VPN, cloud platforms, and endpoints
- Whether access is revoked immediately upon termination
- Backup frequency, retention policies, and off-site storage protections

This shift means carriers no longer accept vague promises of *"security in place"*. They expect detailed answers and the evidence to back them up.

Claims Are Rising, and So Are Underwriting Standards

Today's cyber insurance questionnaires aren't simply asking *"Do you have MFA?"* They ask how it's configured, where it's enforced, and whether you can provide logs or screenshots. **For example:**

These aren't just technical questions; they're operational assessments. While the questions may appear simple, the expected answers require documentation, such as:

- Enforcement policies
- Screenshots of the configuration
- Audit logs showing user activity
- Role-based access reports

In many denials, it's not that the answer was wrong. It's that the answer couldn't be proven.

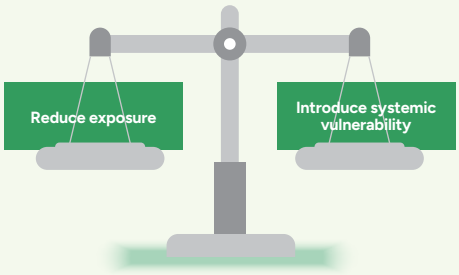
MSPs: Mitigators or Aggregators?

Managed Service Providers (MSPs) face a dual challenge. Not only must they complete insurance applications for their own coverage, but they're often responsible for doing so across multiple client environments.

From a carrier's perspective, this makes MSPs a point of concentration risk. Depending on the quality and consistency of implementation, an MSP can either:

- Reduce exposure across their client base
- Or introduce systemic vulnerability if controls aren't reliably enforced

From a carrier's perspective, a MSP can either:



According to ConnectWise, *"Underwriters are now looking at how MSPs structure and implement security controls for all their clients."* In today's market, there are only 4-5 major cyber underwriters, but they feed millions of broker-buyer transactions. So, what do they want to know?

What Underwriters Are Really Asking

Cyber insurance applications have evolved. What once consisted of broad yes/no prompts has become a direct reflection of the most widely adopted compliance frameworks: NIST 800-171, CMMC Level 2, and HIPAA. While carrier wording may vary slightly, the technical expectations are consistent and increasing.

Common Themes Across Today's Applications

Across nearly all modern cyber insurance forms, from Beazley and CRC Group to QBE NZ and CFC, you'll find questions centered on five key areas:

- Multi-Factor Authentication (MFA)
- Privileged Access Management (PAM)
- Account Deprovisioning & Password Policies
- Logging & Monitoring of Sensitive Systems
- Service Account and Identity Inventory

These are not theoretical inquiries. They're pulled almost verbatim from carrier questionnaires and mirrored in modern compliance programs. To underwriters, security posture is a measurable formula, not a promise.

MFA

It starts with Multi-Factor Authentication (MFA). A simple yes is no longer enough. Underwriters now drill into where MFA is applied and how it's enforced. The Beazley Cyber Insurance Application asks, *"Is MFA required for all remote access (e.g., VPN, RDP, cloud)?"*

Meanwhile, CRC Group presses further: *"Does your MFA cover cloud-based email, firewalls, and remote users?"*

These questions may seem straightforward, but unless you can produce logs, screenshots, or enforcement policies to back up your answers, underwriters may consider your response unverifiable and decline coverage or a future claim.

PAM

Privileged Access Management (PAM) is another focal point. Once viewed as enterprise-only, PAM is now a baseline requirement even for small and mid-sized businesses. As the CRC Group puts it: *"Do you use a privileged access management solution to manage and secure privileged credentials?"*

Some forms go further, asking whether access is time-bound or *"just-in-time,"* a reference to dynamic PAM workflows seen in CMMC and Zero Trust models.

Account Deprovisioning & Password Policies

When it comes to account deprovisioning and password governance, insurers want proof that access doesn't linger after employee offboarding and that password hygiene is enforced. Beazley asks: *"Are access credentials disabled within 24 hours of employee termination?"*

In the CRES Cyber Liability Questionnaire, you'll find requirements for password complexity, expiration policies, and account lockouts after failed login attempts. These controls are foundational, but only if they're verifiable.

Service Account & Identity Inventory

In recent years, carriers have started focusing more on non-human identities. Bots, scripts, and service accounts often have elevated access and few monitoring controls. That's why updated forms like the QBE NZ Cyber Proposal now ask: *"Do you maintain an inventory of service accounts and non-human identities?"*

This aligns with CMMC Level 2 practices 3.5.7 and 3.5.8, which require organizations to identify and manage all types of credentials, not just those tied to human users.

Logging & Evidence of Controls

But perhaps the most critical shift is the growing emphasis on logs and evidence. It's not enough to say your tools are in place. You need to prove they're working. The CRC application includes this direct prompt: *"Do you have the ability to provide logs and audit trails of privileged access?"*

And Coalition's own underwriting guidance spells it out: *"Most ransomware claims we deny aren't about the absence of tools; it's the absence of proof that those tools were working."*- Coalition Inc.

In other words, if your organization has already taken steps toward CMMC or HIPAA alignment, you're likely familiar with these requirements. You're not imagining it. Cyber insurance applications are reading more like compliance audits. If you can't confidently prove every 'yes' with evidence, your answer may be treated as a 'no' at claim time.

When ‘Yes’ Isn’t Enough

Ransomware attacks, social engineering, and supply chain exploits have forced carriers to scrutinize not just what you say, but what you can prove. Incomplete, inaccurate, or unverifiable answers are now one of the leading causes of denied payouts, even when a policy is in place.

> Carriers are increasingly denying claims where controls are claimed but not demonstrable... if you can’t produce logs or documentation, the answer may be treated as a no.”
> — SeedPod Cyber

It’s not just theory. The reality plays out in real-world MSP-client relationships.

> I spoke with an MSP partner whose application missed an MFA requirement, and their client was later denied a ransomware claim. Your answers must be correct, complete, and verifiable.”
> — Stephan Tomecko,
> Director of Partner Success at CyberQP

Even well-intentioned responses can become liabilities. Many forms are submitted with assistance from MSPs, internal IT teams, or brokers. If no one validates the implementation behind the answers, the organization may be left vulnerable when the insurer investigates post-incident.

What “Evidence” Looks Like to an Underwriter

Unlike a compliance audit, insurance underwriting typically doesn’t require documentation upfront. But during a claim investigation, underwriters may request:

- Screenshots of MFA or PAM configuration settings
- Logs of MFA enforcement attempts, access approvals, or system alerts
- Audit trails showing when controls were enabled or bypassed
- Access provisioning reports tied to onboarding/offboarding policies

Forms from carriers such as Beazley, CRC Group, and QBE NZ indicate that evidence may be required either after submission or during a claims audit. What matters is not just whether the control existed, but whether it was enforced and monitored at the time of the breach.

“It’s not enough to say you have MFA. You need to demonstrate that it’s enforced consistently and covers all critical systems.” — ConnectWise

Compliance Meets Coverage

The distinction between a security audit and a cyber insurance application is fading. Today’s underwriters increasingly treat the application itself as a formal attestation, much like a compliance submission.

In both cases, the expectation is clear: If a control isn’t documented, it may as well not exist.

“Controls are no longer abstract checkboxes. If they can’t be shown, they may as well not exist.” — Stephan Tomecko, Director of Partner Success at CyberQP

This convergence has serious implications for MSPs and IT leaders. Applications must be approached not as one-off paperwork, but as a formal risk declaration, backed by technical and administrative evidence.

In the next section, we’ll explore how to prepare for this shift, starting with the tools, policies, and control documentation underwriters expect to see.

Frameworks Drive the Language of Insurance

What many MSPs and internal IT teams don't realize is that most cyber insurance questions are pulled directly from compliance frameworks they already know. Whether or not the carrier explicitly cites it, the technical language in these applications closely mirrors controls from:

CMMC (Cybersecurity Maturity Model Certification)

NIST 800-171 and 800-53

HIPAA Security Rule

"Carriers don't invent these questions. They pull them from frameworks MSPs already use for compliance."
— Stephan Tomecko, Director of Partner Success at CyberQP

This gives security-conscious organizations a strategic advantage. When you understand what a question maps to, and which audit artifact can prove it, you can:

Respond with confidence

Anticipate documentation requests

Reuse existing evidence from audits and security reviews

In short, you don't need to start from scratch. You just need to connect the dots.

Insurance Requirement	Mapped Control	Framework(s)
Enforce MFA across remote/admin access (VPN, RDP, cloud)	IA.1.076 – MFA for network access	CMMC, NIST 800-171, HIPAA
Use PAM for privileged user sessions	AC.2.007 – Privileged access management	CMMC, NIST 800-53, ISO 27001
Revoke access for terminated users within 24 hours	AC.1.001 – Account deactivation	CMMC, NIST, HIPAA
Maintain inventory of service accounts and identities	AC.1.002 / AC-2(3) – Account inventory	CMMC, NIST 800-53
Monitor and log all privileged access and admin actions	AU.2.042 – Audit logging	CMMC, NIST 800-171, HIPAA
Provide policies and evidence that controls are implemented	CA.2.159 – Security documentation	CMMC, NIST

Source: Control names and mappings validated via CyberQP's Shared Responsibility Matrix

Real Application Language That Reflects These Frameworks

CRC Group asks:
"Are access controls in place for all privileged users?"
— Reflects CMMC AC.2.007

CRES Cyber Liability Questionnaire includes:
"Can you provide logs showing security events or incidents?"
— Maps to CMMC AU.2.042 / NIST 800-53 AU-6

Beazley wants to know:
"Do you have policies in place for access control and deprovisioning?"
— Aligned with CMMC AC.1.001 / AC.1.003

Organizations in regulated verticals, like defense (CMMC), healthcare (HIPAA), and finance (GLBA/NIST), may already manage these frameworks. For those teams, insurance readiness is a byproduct of proactive compliance alignment.

CyberQP helps MSPs and internal teams operationalize these requirements to satisfy both auditors and underwriters. Whether you're pursuing CMMC Level 2 or preparing a renewal with Beazley or AmWINS, the control expectations are largely the same.

Why Traditional Tools Can't Prove Coverage

Many MSPs already have a security stack in place: MFA, antivirus, backups, EDR, and even a basic PAM tool. Traditional tools weren't built to satisfy cyber insurance questionnaires or to generate evidence for underwriters. As a result, providers are getting caught off guard when their tech stack fails to meet coverage expectations

Why? Because traditional security products were designed to block threats, not prove controls. Underwriters don't want to hear that a feature exists. They want to see the audit logs, policy details, and access records that show how it was used, enforced, and monitored.

Even when controls are technically present, MSPs still face the burden of operationalizing them across multiple client environments.

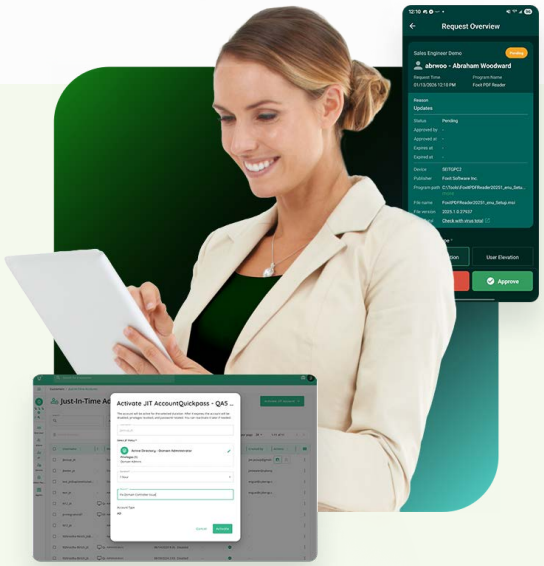
That means:

- Aggregating multiple tools to answer a single insurance question
- Generating custom screenshots, logs, and policies
- Manually mapping tool outputs to frameworks like CMMC
- Explaining technical controls in business terms a broker or underwriter will accept

"It's the same work, the same questions, over and over. Clients pass it off to their MSP, who has to fill out the application with no clear tools to answer confidently."
— Stephan Tomecko, Director of Partner Success at CyberQP

Where the Gaps Show Up in Typical Tools

Typical Tool	What's Missing for Insurance
Endpoint Detection & Response (EDR)	Doesn't prove privileged account separation or MFA enforcement
Basic MFA Platform	Doesn't log enforcement scope or link to RDP/VPN systems
Directory Services / RMM	No audit logs tied to access policies or deprovisioning events
Off-the-shelf PAM	Lacks framework mappings, tenant scalability, or evidence export



The CyberQP Approach

CyberQP wasn't built to be just another security tool. It was designed from the ground up to bridge the gap between control enforcement and proof of compliance, specifically for the types of requirements appearing in today's cyber insurance applications.

Traditional tools focus on functionality. CyberQP focuses on accountability.

It doesn't just enforce identity and access policies. It documents them in a way that underwriters, auditors, and compliance teams can verify. Whether you're an MSP managing dozens of tenants or an internal IT team responsible for passing an audit or securing a renewal, CyberQP translates your operational controls into defensible evidence.

Unlike most legacy security vendors, CyberQP understands the language of risk, not just security.

Identity and Access, Ready for Audit

CyberQP combines multiple security and compliance capabilities into a single platform:

- Built-in MFA for privileged access across RDP, VPN, and directory services
- Privileged Access Management (PAM) workflows mapped directly to CMMC and NIST 800-171
- Inventory and oversight of non-human service accounts
- Audit logs capturing access events, password usage, and control activation
- Exportable policy documentation, pre-mapped to frameworks like HIPAA and NIST

These aren't theoretical features. They're practical, repeatable controls designed for proof, not just presence.

Clarity with the Shared Responsibility Matrix

One of CyberQP's most powerful differentiators is its CMMC Shared Responsibility Matrix, a mapped accountability framework that defines which party (MSP or client) is responsible for each control.

This matrix helps:

- Protect MSPs from assuming full liability during policy attestations
- Clarify ownership for brokers, underwriters, and auditors
- Deliver consistency in answers across client environments

Whether you're completing an AmWINS form, navigating Beazley's coverage tiers, or supporting a CMMC audit, the Shared Responsibility Matrix ensures your responses are consistent, defensible, and tied to real-world control ownership.

Compliance Alignment at Scale

CyberQP is purpose-built to align with:

- CMMC Level 2 requirements
- NIST 800-171 controls
- HIPAA Security Rule safeguards

This alignment reduces the need for costly third-party consultants or one-off documentation exercises. For MSPs, the platform's multi-tenant architecture means that once controls are mapped, they can be:

- Applied consistently across all clients
- Used to generate proof packages for insurance applications and renewals
- Maintained without rework or ad hoc data collection

In short, CyberQP turns compliance alignment into a strategic advantage, not a scramble.

How to Prepare Your Next Application

Cyber insurance is not a safety net. It's a contract with conditions. A signed policy is only as strong as the accuracy and verifiability of the answers provided during the application process.

Insurers are increasingly denying claims due to misstatements, incomplete answers, or missing evidence. The gaps don't have to be malicious to be costly. They just have to be unverifiable.

This section illustrates how minor oversights in identity or access controls can have significant business consequences, particularly for MSPs serving multiple clients.

How Small Mistakes Create Big Risks

In CRC Group's full cyber insurance application, applicants are asked:

"Are user accounts disabled within 24 hours of termination?"

It's a simple yes-or-no, but answering "yes" without supporting documentation can backfire.

According to SeedPod Cyber, a real-world ransomware claim was denied when a contractor's credentials remained active for weeks after their engagement ended. Though the application indicated that termination controls were in place, the absence of logs proved otherwise. The unused account was later compromised and leveraged in a phishing campaign that led to ransomware deployment.

"The claim was denied. The application had answered 'yes' to the termination question, but logs showed no enforcement." — SeedPod Cyber

Coalition, a leading cyber insurer, echoes this concern:

"Most ransomware claims we deny aren't about the absence of tools; it's the absence of proof that those tools were working." — Coalition Inc.

Even when controls like MFA or PAM are technically deployed, failure to log enforcement, document policy, or show configuration timelines can result in denied payouts.

Shared Controls, Shared Liability

For MSPs, the stakes are even higher. When service providers complete insurance applications on behalf of clients, they may be asked to certify the answers. If the controls described aren't properly divided, or worse, misrepresented, it's not just coverage that's denied. It's liability that's shared.

This is where CyberQP's Shared Responsibility Matrix plays a critical role. By clearly identifying which party, MSP or client, is responsible for each control, it:

- Protects MSPs from assuming blanket liability
- Clarifies control ownership for both parties
- Helps underwriters and auditors see a transparent security model

With growing regulatory pressure and rising breach costs, this level of clarity isn't just a best practice. It's a necessity.

The Business Impact of a Denied Claim

A denied cyber insurance claim doesn't just affect the incident in question. It can have long-term ripple effects, including:

- Out-of-pocket costs for breach response and recovery
- Loss of client trust and damaged reputation
- Legal exposure due to inaccuracies or omissions on the application

For MSPs, these issues can jeopardize relationships with multiple clients, especially if they appear responsible for incomplete or incorrect answers. In some cases, it may even open the door to legal action or contract disputes.
Cyber insurance readiness isn't just about compliance. It's about credibility. CyberQP ensures that what you say on the form is exactly what you can prove when it matters most.

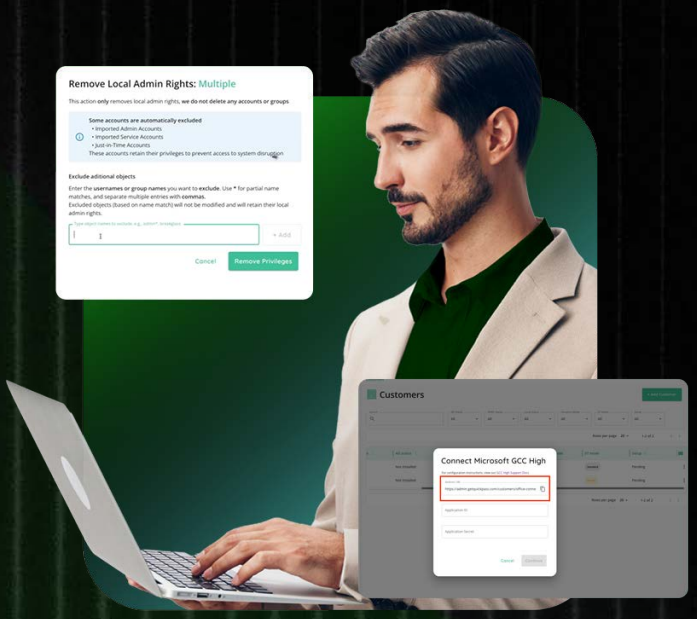
Summary

Whether you're completing your first application or preparing for a renewal, CyberQP helps ensure your answers are not only accurate but also verifiable. From privileged access management to audit-ready evidence, we bridge the gap between security frameworks and real insurance requirements.

Don't wait until an underwriter or a breach exposes the gaps.

Get the Tools to Prove You're Ready:

- → Download the CyberQP CMMC Shared Responsibility Matrix to map control ownership across your environment.
- → Book a 15-minute consultation to review your application readiness and identify high-risk gaps.
- → See how CyberQP supports MFA, PAM, and audit evidence in one platform, built for MSPs and regulated organizations.



Schedule a call today

Glossary

Access Controls

Security measures that restrict access to systems, applications, or data based on a user's identity or role. Strong access controls reduce the chance of unauthorized activity and are required by most cyber insurance carriers.

Audit Trail

A record of who accessed what, when, and how. Underwriters and auditors use audit trails to verify that security controls are enforced and consistently monitored.

CMMC (Cybersecurity Maturity Model Certification)

A U.S. Department of Defense framework that defines cybersecurity standards for contractors and their service providers. Level 2 includes over 100 practices that align with NIST 800-171 and often mirror insurance requirements.

Cyber Liability Insurance

A policy that helps businesses cover the cost of cyberattacks, data breaches, and related disruptions. Coverage depends on meeting and proving specific security control requirements.

Deprovisioning

The process of removing access when a user leaves the company or no longer needs access to a system. Delayed or incomplete deprovisioning is a common cause of breaches and insurance claim denials.

Evidence of Controls

Documentation or logs that prove security measures are in place and functioning. Examples include screenshots, system logs, access policies, or audit reports. Lack of evidence can lead to denied coverage.

Framework Mapping

The process of aligning technical controls with formal frameworks like CMMC, NIST, or HIPAA. CyberQP automates this mapping to streamline audits and insurance applications.

Identity Verification

Confirming that the person requesting access is who they claim to be, typically using MFA or secure workflows. This is foundational for privileged access and required in nearly all cyber insurance applications.

Least Privilege

A principle that limits users to only the access they need, nothing more. Enforcing least privilege is a top control in both compliance and cyber insurance frameworks.

MFA (Multi-Factor Authentication)

A security measure that requires more than one method of verification to access a system. Insurance carriers often require MFA for remote access, email, VPN, RDP, and privileged accounts.

PAM (Privileged Access Management)

Technology that secures and governs accounts with elevated permissions. PAM is essential for managing admin credentials and is a frequently cited insurance requirement.

Proof of Compliance

Clear, documented evidence that a business meets cybersecurity standards. While security tools may provide protection, insurance carriers want assurance that protection is consistent and measurable.

Ransomware

Malicious software that locks or steals data and demands payment for its release. Many cyber insurance policies specifically address ransomware, if security controls like MFA and backups are in place.

Shared Responsibility Matrix

A tool used to define which party, MSP or customer, is accountable for each control. CyberQP's matrix simplifies insurance applications by assigning ownership and reducing liability confusion.

Appendix

The Questions You'll Be Asked and How to Answer Them

These questions are pulled directly from real cyber insurance applications. Underwriters don't just want "yes" or "no" answers—they want evidence. Use this checklist to ensure your security posture is ready and provable.

Insurance Question	How to Check the Box with CyberQP
Do you require MFA for all remote and privileged access, including VPN, RDP, and cloud resources?	**Yes** CyberQP enforces MFA for privileged accounts across Active Directory, Entra ID, and local Windows admin accounts.
Do you use Privileged Access Management (PAM) tools to protect admin accounts?	**Yes** CyberQP applies zero trust principles, including just-in-time access, time-bound tokens, full logging, and rotation after every use.
Do non-IT users have local admin rights on their endpoints?	**No** CyberQP removes standing local admin rights and provides just-in-time elevation with approvals through QDesk.
Are Domain Administrators configured with unique, random, long passwords?	**Yes** CyberQP issues unique MFA tokens for each session, eliminating the risk of password reuse.
Do you restrict access to sensitive systems based on job function?	**Yes** CyberQP restricts access to privileged systems using policy-based access tied to identity and role.
Can you verify all of this with documentation and logs?	**Yes** CyberQP provides audit-ready evidence aligned with CMMC, NIST, and HIPAA frameworks, plus a Shared Responsibility Matrix for MSPs.

The following questions are pulled from actual insurance underwriter forms. This appendix provides a simple guide to answering them precisely.

Beazley Questionnaire

Question	Insurer/Input	Section	How to answer on application (Assuming product is configured and deployed)	Context	Product
Do you require multi-factor authentication (MFA) for all users remote access to the network?	Beazley Questionnaire (short)	Cybersecurity Controls	Yes	CyberQP just-in-time access enforces MFA for Active Directory, Entra ID and Local Windows Administrator privileged access to the network. Customers would require MFA enforcement for end-users (non-privileged users) from another IAM product.	QGuard
Do you require Multi-Factor Authentication (MFA) for remote access to your network (both cloud-hosted and on premises, including via Virtual Private Networks (VPNs)?	Beazley Questionnaire (full)	7	Yes	CyberQP just-in-time access enforces MFA for Active Directory, Entra ID and Local Windows Administrator privileged access to the network. Customers would require MFA enforcement for end-users (non-privileged users) from another IAM product.	QGuard
Do you enforce MFA for privileged accounts in Azure Active Directory (AAD) (including the members of the AAD Domain Controller administrators group)?	Beazley Questionnaire (full)	9.a.	Yes	CyberQP just-in-time access enforces MFA for Active Directory, Entra ID and Local Windows Administrator privileged access to the network. Customers would require MFA enforcement for end-users (non-privileged users) from another IAM product.	QGuard
Are Domain Administrators configured with unique, random, and long (>25 characters) passwords?	Beazley Questionnaire (full)	9.c.	No	CyberQP uses token based MFA on privileged access accounts which is rotated after every use.	QGuard
Do you permit ordinary users local administrator rights to their devices (e.g., laptops)?	Beazley Questionnaire (full)	21	Yes	CyberQP removes standing admin access for end users on enrolled endpoints and provides controls and approvals for just in time elevation of admin privileges when required.	QDesk

Tokio Marine HCC Netguard Plus

Question	Insurer/Input	Section	How to answer on application (Assuming product is configured and deployed)	Context	Product
Is Multi-Factor Authentication (MFA) enforced to secure all remote access to your network for all employees and third parties on all applications, including VPNs (Virtual Private Network), RDP (Remote Desktop Protocol), RDWeb (Remote Desktop Web) or any RMM (Remote Management and Monitoring) applications?	Tokio Marine HCC Netguard Plus	7.a.2	Yes	CyberQP just-in-time access enforces MFA for Active Directory, Entra ID and Local Windows Administrator privileged access to the network. Customers would require MFA enforcement for end-users (non-privileged users) from another IAM product.	QGuard
Select your MFA type: Choose an item.	Tokio Marine HCC Netguard Plus	7.2	Other	CyberQP uses token based MFA on privileged access accounts which is rotated after every use.	QGuard
If "Other", describe your MFA type: _____	Tokio Marine HCC Netguard Plus	7.2	CyberQP uses token based MFA on privileged access accounts which is rotated after every use.	CyberQP uses token based MFA on privileged access accounts which is rotated after every use.	QGuard
Do you require MFA to protect all local and remote access to privileged user accounts?	Tokio Marine HCC Netguard Plus	7.d	Yes	CyberQP just-in-time access enforces MFA for Active Directory, Entra ID and Local Windows Administrator privileged access to the network. Customers would require MFA enforcement for end-users (non-privileged users) from another IAM product.	QGuard
Select your MFA type: Choose an item.	Tokio Marine HCC Netguard Plus	7.d	Other	CyberQP uses token based MFA on privileged access accounts which is rotated after every use.	QGuard
If "Other", describe your MFA type: _____	Tokio Marine HCC Netguard Plus	7.d	CyberQP uses token based MFA on privileged access accounts which is rotated after every use.	CyberQP uses token based MFA on privileged access accounts which is rotated after every use.	QGuard

Traveler's Cyber Risk Application

Question	Insurer/Input	Section	How to answer on application (Assuming product is configured and deployed)	Context	Product
Indicate whether the Applicant currently has the following in place: Multi-factor authentication for administrative or privileged access	Travelers Cyber Risk Application	7.h	Yes	CyberQP just-in-time access enforces MFA for Active Directory, Entra ID and Local Windows Administrator privileged access to the network. Customers would require MFA enforcement for end-users (non-privileged users) from another IAM product.	QGuard
Indicate whether the Applicant currently has the following in place: Restricted access to sensitive data and systems based on job function	Travelers Cyber Risk Application	6.f	Yes	CyberQP restricts access to sensitive data and systems for Privileged Accounts in the Microsoft stack. Customers would require access restrictions on other accounts from another IAM product.	QGuard
Indicate whether the Applicant currently has the following in place: Multi-factor authentication for remote access to the Applicant's network and other systems and programs that contain private or sensitive data in bulk	Travelers Cyber Risk Application	7.i	Yes	CyberQP just-in-time access enforces MFA for Active Directory, Entra ID and Local Windows Administrator privileged access to the network. Customers would require MFA enforcement for end-users (non-privileged users) from another IAM product.	QGuard

Apogee Questionnaire

Question	Insurer/Input	Section	How to answer on application (Assuming product is configured and deployed)	Context	Product
Does the policyholder enforce Multi-Factor Authentication (MFA) for all employees, contractors, and partners, in addition to cloud deployments, email, mission-critical systems, privileged accounts, VPN, and remote access?	Apogee Questionnaire	20	Yes	CyberQP just-in-time access enforces MFA for Active Directory, Entra ID and Local Windows Administrator privileged access to the network. Customers would require MFA enforcement for end-users (non-privileged users) from another IAM product.	QGuard

Victor Cyber Insurance

Question	Insurer/Input	Section	How to answer on application (Assuming product is configured and deployed)	Context	Product
Please confirm whether multi-factor authentication is required for all remote access to your network.Monitoring) applications?	Victor Cyber Insurance	35	Yes	CyberQP just-in-time access enforces MFA for Active Directory, Entra ID and Local Windows Administrator privileged access to the network. Customers would require MFA enforcement for end-users (non-privileged users) from another IAM product.	QGuard
If you use an alternative method for securing remote access to your network, such as certificate-based authentication for devices, please provide details:	Victor Cyber Insurance	36	CyberQP uses token based MFA on privileged access accounts which is rotated after every use.	CyberQP uses token based MFA on privileged access accounts which is rotated after every use.	QGuard
Please confirm whether multi-factor authentication is required to access all cloud resources holding sensitive or confidential information:	Victor Cyber Insurance	37	Yes	CyberQP just-in-time access enforces MFA for Active Directory, Entra ID and Local Windows Administrator privileged access to the network. Customers would require MFA enforcement for end-users (non-privileged users) from another IAM product.	QGuard
Please provide details on how you protect privileged user accounts (e.g., using privileged access management solutions, restricting privileged user accounts to specific devices, enhanced monitoring of accounts for anomalous usage, multi factor authentication enabled for remote access, etc.):	Victor Cyber Insurance	42	CyberQP enforces a zero trust approach to privileged user accounts. Rotated tokens after each use, time bound access, MFA, and full logging.	CyberQP enforces a zero trust approach to privileged user accounts. Rotated tokens after each use, time bound access, MFA, and full logging.	QGuard
Do non-IT users have local administrator rights on their laptops/desktops?	Victor Cyber Insurance	43	No	CyberQP removes standing admin access for end users on enrolled endpoints and provides controls and approvals for just in time elevation of admin privileges when required.	QDesk

Northbridge Cyber Application

Question	Insurer/Input	Section	How to answer on application (Assuming product is configured and deployed)	Context	Product
Is there an online multifactor authentication method required to access company sensitive data?	Northbridge Cyber Application	15.i	Yes	CyberQP just-in-time access enforces MFA for Active Directory, Entra ID and Local Windows Administrator privileged access to the network. Customers would require MFA enforcement for end-users (non-privileged users) from another IAM product.	QGuard

Cyberboxx Insurance Application

Question	Insurer/Input	Section	How to answer on application (Assuming product is configured and deployed)	Context	Product
Please select the security measures that the Applicant has in place: Multi-factor Authentication	Cyberboxx Insurance Application	Please select the security measures that the Applicant has in place:	On remote access to the network On privileged accounts	CyberQP just-in-time access enforces MFA for Active Directory, Entra ID and Local Windows Administrator privileged access to the network. Customers would require MFA enforcement for end-users (non-privileged users) from another IAM product.	QGuard

CFC Corporate Cyber

Question	Insurer/Input	Section	How to answer on application (Assuming product is configured and deployed)	Context	Product
Please confirm whether multi-factor authentication is required for all remote access to your network.	CFC Corporate Cyber	6.5.	Yes	CyberQP just-in-time access enforces MFA for Active Directory, Entra ID and Local Windows Administrator privileged access to the network. Customers would require MFA enforcement for end-users (non-privileged users) from another IAM product.	QGuard
Please confirm whether multi-factor authentication is required to access all cloud-based resources where you store confidential and sensitive data.	CFC Corporate Cyber	6.7.	Yes	CyberQP just-in-time access enforces MFA for Active Directory, Entra ID and Local Windows Administrator privileged access to the network. Customers would require MFA enforcement for end-users (non-privileged users) from another IAM product.	QGuard
Please describe how you protect privileged user accounts. Please include details on any use of internal multi-factor authentication and/or privileged access management tools:	CFC Corporate Cyber	6.8.	CyberQP enforces a zero trust approach to privileged user accounts. Rotated tokens after each use, time bound access, MFA, and full logging.	CyberQP enforces a zero trust approach to privileged user accounts. Rotated tokens after each use, time bound access, MFA, and full logging.	QGuard
Do your non-IT users have administrative rights on their laptops/ desktops?	CFC Corporate Cyber	6.9.	No	CyberQP removes standing admin access for end users on enrolled endpoints and provides controls and approvals for just in time elevation of admin privileges when required.	QDesk