CyberQP

How Passwordless JIT Helps IT and Security Professionals Meet **Cyber Insurance Requirements**

Legislators and cyber insurance providers have noticed the major (and growing role) privileged access plays in cyber insurance.

In response, they have introduced requirements that businesses and their IT or security partners implement additional security controls around their privileged accounts, including **Multi-Factor Authentication (MFA)**.

At the same time, several cybersecurity thought leaders and experts are questioning the role passwords play in today's digital landscape. Are they obsolete security risks, or can users still trust passwords as "something you know" for authentication?

Here's an in-depth look at the best practices for privileged access management today, and how Managed Service Providers and help desks can build and execute on an identity security strategy that helps businesses stay resilient in today's threat landscape.

Stolen credentials have appeared in

31%

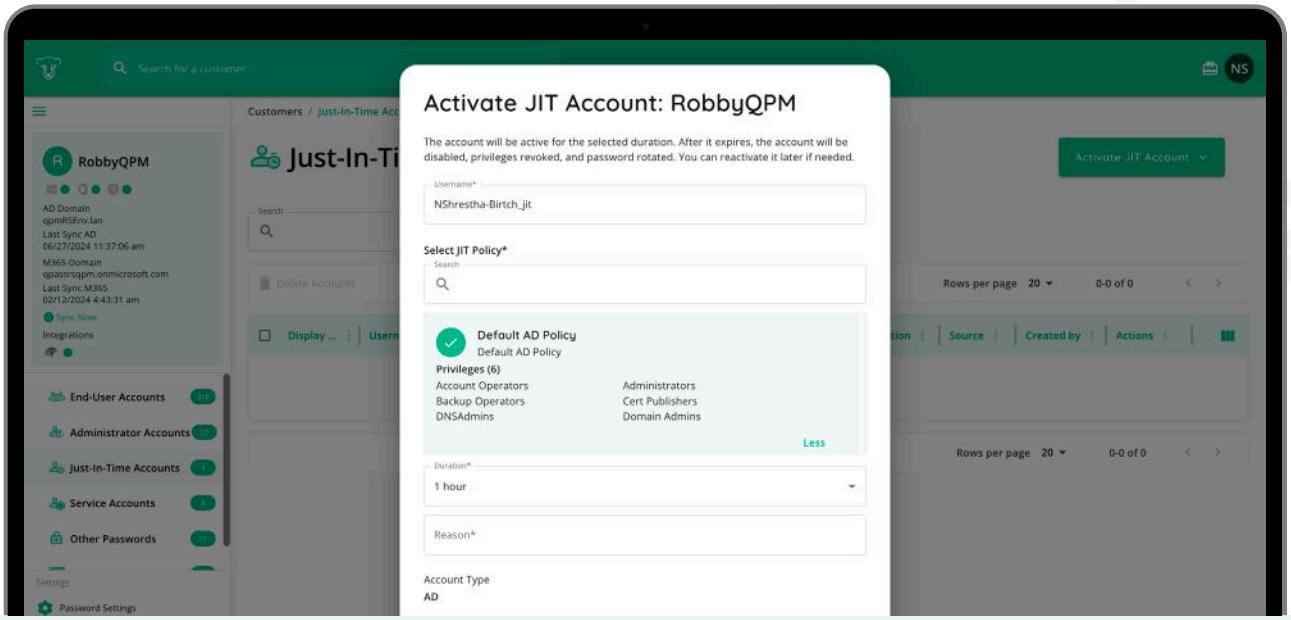
of breaches over the past 10 years.

Verizon Data Breach Investigations Report 2024

Cyber Insurance Requirements

When the CyberQP team analyzed publicly available cyber insurance eligibility questionnaires, we saw that cyber insurance providers aren't just asking for traditional **Identity and Access Management (IAM)** or **Privileged Access Management (PAM)** solutions in a business' security program anymore.

Here's what we found:



Secure Privileged Access with Multi-Factor Authentication

Cyber insurance providers' most common eligibility requirement involving privileged access is the enforcement of MFA around all privileged accounts. For example, Chubb, a major cyber insurance provider, requires MFA for "internal or on-network [privileged] access."

In fact, providers will even have granular eligibility requirements per directory source. For example, Beazley asks potential clients if they enforce MFA for privileged accounts in Microsoft Entra ID (formerly Azure Active Directory), including domain administrator accounts, and Chubb will ask about service accounts.

Monitor Administrator Access Regularly

In our analysis, we also found several providers (Axis Capital & Chubb) require regular monitoring of privileged accounts, whether it's on a weekly, monthly, or quarterly basis. Moreover, providers will also require the ability to audit privileged access and activity as needed.

Separate Privileged Accounts Per Employee

Moreover, these questionnaires also ask whether an organization is separating non-privileged access from privileged accounts, including "separate logins, passwords, and authentication."

Looking Ahead at Future Requirements & Best Practices

While cyber insurance requirements don't directly require MSPs to achieve and enforce **Zero Standing Privileges**, providers are guiding prospective clients towards ZSP.

Specifically, when Chubb asks how many privileged accounts an organization uses, they also offer a field for commentary on how they plan to reduce the number of persistent administrator accounts.

Moreover, providers are also concerned about lateral movement attacks – which is why they're asking about least privilege access controls.

How MSPs Can Build a PAM Strategy

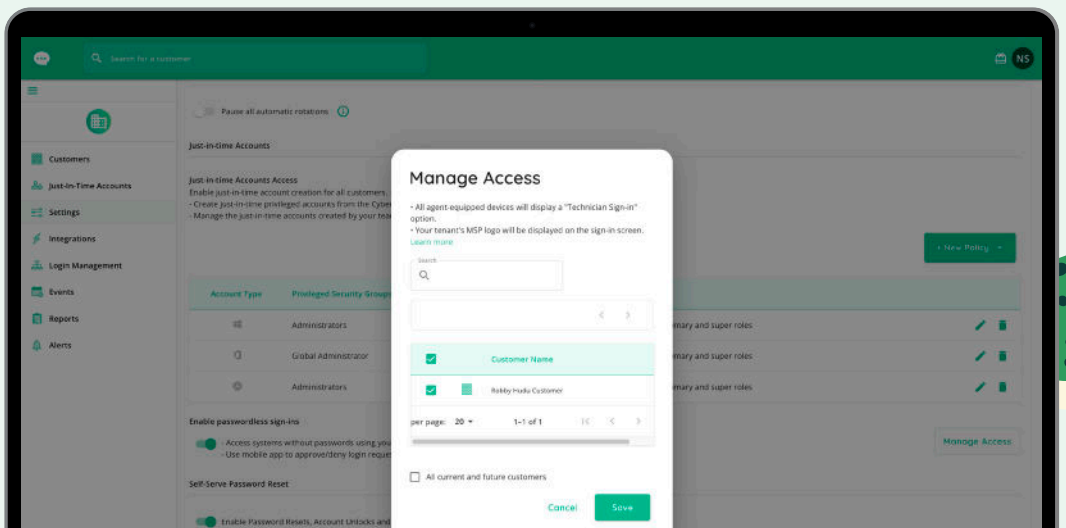
and Prepare for Cyber Insurance Conversations

CyberQP is prepared to help MSPs and help desks meet these cyber insurance requirements, prepare for discussions with cyber insurance providers, and have conversations about why their end users need to adopt proactive security measures.

Using QGuard Pro, CyberQP Partners can issue unique Just-in-Time accounts per technician to replace persistent admin accounts and only offer privileged access when a technician needs it.

MSPs can also go one step further with Passwordless JIT Access for Technicians, which enables MSPs to secure their endpoints and servers by adding a dedicated MFA challenge and eliminating password interactions. Achieve a competitive edge in compliance management.

Technicians can also use the CyberQP dashboard to enforce a culture of accountability with clean audit logs.



How **QGuard Pro** Accelerates Privileged Logins and Follows Least Privileges

QGuard Pro plays a pivotal role in safeguarding an organization's critical assets against the following security threats.

Credential Stuffing Attacks

When a threat actor launches a credential stuffing attack, MSPs can use QGuard Pro to reduce or eliminate the amount of time a privileged account is vulnerable for, with rotating credentials, Just-in-Time access, and Passwordless MFA logins.

Malware and Ransomware

Malware and ransomware variants frequently target Active Directory and privileged accounts. By limiting privileged access, QGuard Pro limits the amount of lateral movement a threat actor can potentially take during an incident.

Insider Threats

Even trusted insiders can misuse privileges. QGuard Pro enables MSPs to monitor for new privileged accounts and establish time limits on admin access with JIT accounts to prevent misuse.

When techs are assigned a ticket that requires privileged access, they need a quick and secure way to get that access.

Technicians can use CyberQP's Passwordless MFA to save 30-45 seconds per privileged account login.

With QGuard Pro, our partners can get admin access on-demand, only when they need it - achieving zero standing privileges.

TECHNICIAN NEEDS PRIVILEGED ACCESS → **PROVISION TEMPORARY ADMIN ACCESS** → **ACCELERATE PRIVILEGED LOGINS** → **DISABLE AUTOMATICALLY** → **AVAILABLE WHENEVER YOU NEED IT**

Techs can use the CyberQP dashboard or the Tech mobile app to create a unique Just-in-Time account and set a time limit for their privileged access.

Once a technician finishes their work, QGuard Pro automatically disables the JIT account, strips it of its admin privileges, and rotates its credentials.

Are you ready to reduce your attack surfaces and make it easy to provision privileged access for a limited amount of time, and for specific technicians?

MSPs can book a demo today to see how they can follow best practices for privileged access management.

Works Cited:

Chubb ERM Questionnaire:
https://www.chubb.com/content/dam/chubb-sites/chubb-com/uk-en/business/by-category-cyber-enterprise-risk-management/documents/pdf/11100c_chubb_cyber_erm_standard_proposal_form.pdf

Beazley Cyber Insurance Application:
https://www.beazley.com/globalassets/product-documents/application/beazley_cyber_insurance_application_above_250m.pdf