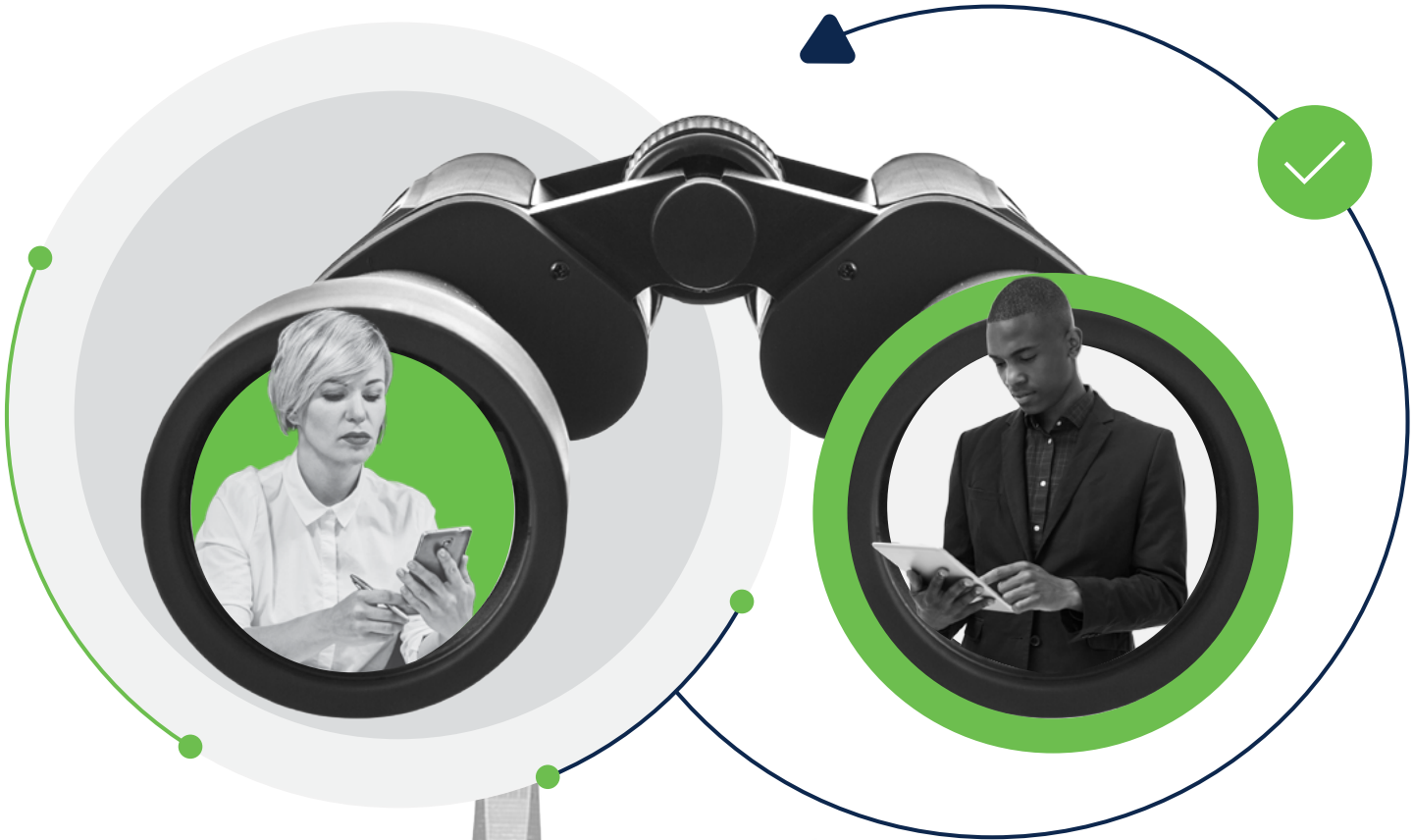
Cyber Liability Insurance

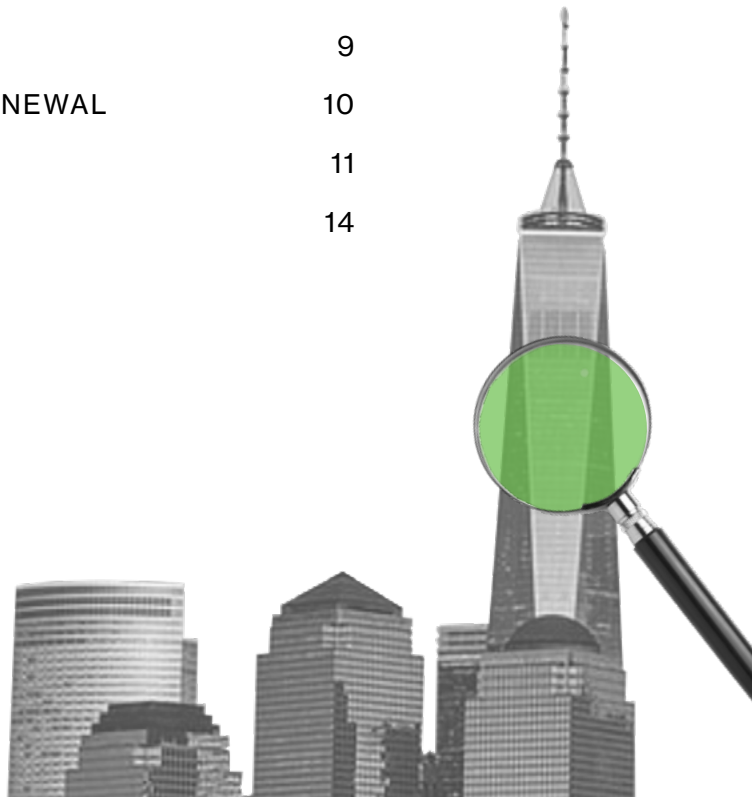
WHAT YOU NEED TO KNOW



Cyber Liability Insurance

WHAT YOU NEED TO KNOW

CONTENTS



How Does Cyber Liability Insurance Work?

Cyber liability insurance can be a lifeline in the event of a major incident or breach. Cyber incidents rose 35% in 2020 alone with data breaches costing $4.24 million per year, resulting in cyber insurance premiums jumping up by 50-100%. Modern challenges like phishing, ransomware, remote workforces, stolen credentials and personal devices demand increasingly sophisticated cybersecurity practices. Organizations must secure themselves against unknown and advancing threats while striking a balance between proactive and reactive measures. No doubt, cyber insurance is a hot topic right now. Do you need it? How do you qualify for it? How much will it cost?

Like health and car insurance, cyber insurance is a line of coverage designed to mitigate losses from cyber incidents. Organizations may suffer data breaches, network damage, stolen backups, reputational damage and the disruption of daily operations. Multi-factor authentication (MFA), endpoint visibility and access controls like Duo provides are often required and can mitigate these risks and lower insurance rates. The unfortunate reality is that cyber insurance is becoming a necessity for organizations big and small. It's no longer a question of whether you should buy cyber insurance and what it covers. It is now how much of this insurance should you buy? And what security practices do you need to put in place to qualify?

While each provider's policy may differ slightly, cyber liability insurance generally deals with:

- Loss or destruction of data
- Damage to software/hardware
- Extortion demands to appease bad actors
- Breach incident response and crisis management
- Legal claims for defamation, fraud and privacy violations (third-party coverage)

How Cyber Insurance Helps

Software exploits continue to be the leading cause of data loss. Some of the things cyber insurance can do for you in the event of an incident are:

Notify impacted parties and monitor their credit.

Evaluate and fix any security flaws, replace income from system downtime.

Hire a PR agency to manage reputational damage and coach you on the best way to handle and communicate the situation to your customers and the public.

Recover expenses to continue business operations so you can get back and running.

The Playing Field Has Changed

Insurance companies today are focused on a company's ability to prevent, mitigate and respond to ransomware attacks. It's all driven by losses.

Most insurance companies have been struggling for the past two years to be profitable writing cyber insurance policies. Some of the top leaders in the cyber insurance space wrote coverage at a loss. Insurance companies' loss ratios for cyber insurance -- how much is paid in premiums versus how much is paid out in claims -- worsened by nearly a third in 2020 compared to the previous year, according to a report by the National Association of Insurance Commissioners (NAIC).

This puts pressure on cyber insurance pricing. Previous actuarial modeling did not account for ransomware losses. Even with ransomware factored into pricing, attacks kept growing in frequency and severity to the point where insurance companies had a hard time keeping up with it. There was a ransomware victim every 10 seconds in 2020, and according to a recent survey one in five Americans are victims of ransomware.

Why Premiums Are Increasing

A major factor right now in price increases is that these can be fast moving claims. "With a ransomware claim, an insurance company could be out of full limit loss (the maximum amount offered) in a week. Insurance companies could be out a full limit loss in a night if a ransom demand is high enough," said Cole Haney, assistant vice president, professional and cyber practice at Hays Companies, a risk management and cyber insurance provider.

Ransomware is hitting companies of all sizes, something that has been a huge change for insurance carriers. Historically in cyber, data breaches are responsible for most of the large losses. Data breaches take years to play out – there's liability, class action lawsuits, regulatory fines, penalties, and investigations – things that take a long time. It gives insurance companies more time to factor that into the pricing.

But when things move fast, that's where insurance companies have a hard time keeping up. They have to constantly adjust the coverage pricing. Unfortunately, that pricing is increasing drastically for nearly everyone.

“

I’d say multi-factor authentication is what’s going to mostly determine your ability to purchase cyber insurance.”

Cole Haney, assistant vice president, professional and cyber practice at Hays Companies.

Insurers’ Risk Evaluation

Many companies have been affected by how rapidly the insurance companies change the cyber evaluation process. Cyber insurance providers went from a very loose approach, where they mainly analyzed basic company information, to a more strict and technical approach, where cybersecurity, and particularly ransomware protection, is now top of mind. In the past, security practices like multi-factor authentication typically meant a discount on premiums but now it is often a baseline requirement. Cyber insurance companies are taking a closer look at risk and evaluating it prior to issuing coverage.

Is your organization specifically a valuable target? And what makes you a valuable target or not? What kind of data do you collect? Do you have a lot of customer data that could be damaging and result in identity theft? Are attackers actually able to steal actual money from people? How are you storing that data and who has access to it? What kind of security practices do you have in place and how do you enforce them? Insurance companies today are focused on a company's ability to prevent, mitigate, and respond to ransomware attacks.

The ability to obtain coverage is increasingly dependent on cyber hygiene. Here is a snapshot of the most critical items today that insurance companies frequently want you to have.

Key Security Measures For Coverage

Multi-Factor Authentication

- Remote access to network
- Remote access to email
- Privileged user access
- Encrypted backups
- Device trust

Data Backup & Recovery

- Regularly scheduled
- Tested restoration
- Encrypted & separate from network (offline/air-gapped)
- Incident response & Disaster recovery planning

Additional controls of concern:

- Patching cadence
- Endpoint Detection & Response tool implemented
- Employee training
- Email filtering & validation process
- Privileged account management (PAM) software

These practices go into a strong security strategy that insurance companies are looking for. To determine what coverage is necessary, cyber liability insurers calculate cost based on a variety of risk factors. Often among them are industry, data coverage and, most importantly, the security measures already in place. These providers want to ensure the clients are taking fundamental safety measures to protect its systems and users.

One common basic requirement is multi-factor authentication for secure access to validate the user's identity and help defend against account compromise. Much more than merely one more box in the insurance requirement checklist, choosing the right MFA solution for the modern hybrid or cloud environment can lay the foundation for shifting security strategy from reactive to proactive.

> One market leader said from analyzing claims in 2020 that over 90% of its policyholders that experienced a ransomware loss did not have multi-factor authentication in place.

What Affects Your Rate

Multi-Factor Authentication

You will notice multi-factor authentication is at the top of the list of typical requirements to qualify for cyber insurance. The degree to which multi-factor authentication needs to be used can vary by insurance company and sometimes the size of the client. However, nearly all are going to require it for remote access to the network, email on web applications, and access to administrative accounts. Insurers also look to see if MFA is used for backups and logging into cloud services for mid-to-large sized companies.

"What I would consider the most critical items today during the evaluation process first and foremost begins with multi-factor authentication at this point. It is required by essentially all insurers in this space to get insurance" — Cole Haney, assistant vice president, professional and cyber practice at Hays Companies.

Carriers used to be more flexible. Some would offer coverage if a client agreed to implement MFA at a later date, but now it has to be in place before coverage can take effect. MFA is the first step to a zero trust posture. "Trust no one, continuously verify" is the core tenet of zero trust. By limiting access to only specific authorized users and having policy controls, MFA is effective at preventing stolen credentials and access to networks.

> A zero trust layered Virtual Private Network (VPN) and firewall approach that includes MFA prevents 100% of automated bots, 99% of bulk phishing attacks and 90% of targeted attacks, according to Google research.

Protecting Backups

After MFA, protecting backups is a key practice that insurers look at when evaluating risk. If bad actors aren't able to reach your secondary data copies, it's very unlikely that the insurance company is going to have to pay for the policyholder to submit a ransom demand, or pay for a full system rebuild. With backup security, the carriers prefer to see clients that use separate networks to store the data, keep the backups offline, encrypt their backups, and use MFA to gain access. Insurers consider having these best-in-class practices in place to reduce risk.

Insurers typically also want confirmation that companies test the restoration of the backups. "It's actually what led to the largest demand payment that I have personally seen. I had a client that was under a ransomware attack. They had really secure backups, they were essentially untouched. But they found out during the attack that their systems were not configured correctly. And so, when they went to actually restore their data, it didn't work, it didn't copy over correctly, and they weren't able to get their environment back in place," Haney said. The company had never practiced restoring their backups and had to submit an eight-figure demand to get their computer systems back. Often insurers want to see if you test your fail safes because it could cost them if you do not.

Finally, insurers frequently require you to have a documented scenario-based response plan and that you actually test it. Your response plan should consider scenarios such as ransomware attacks, device compromise and insider threats, as well as how your organization would respond to them, especially in today's environment where there is a large remote workforce.

Patching Systems and Updates

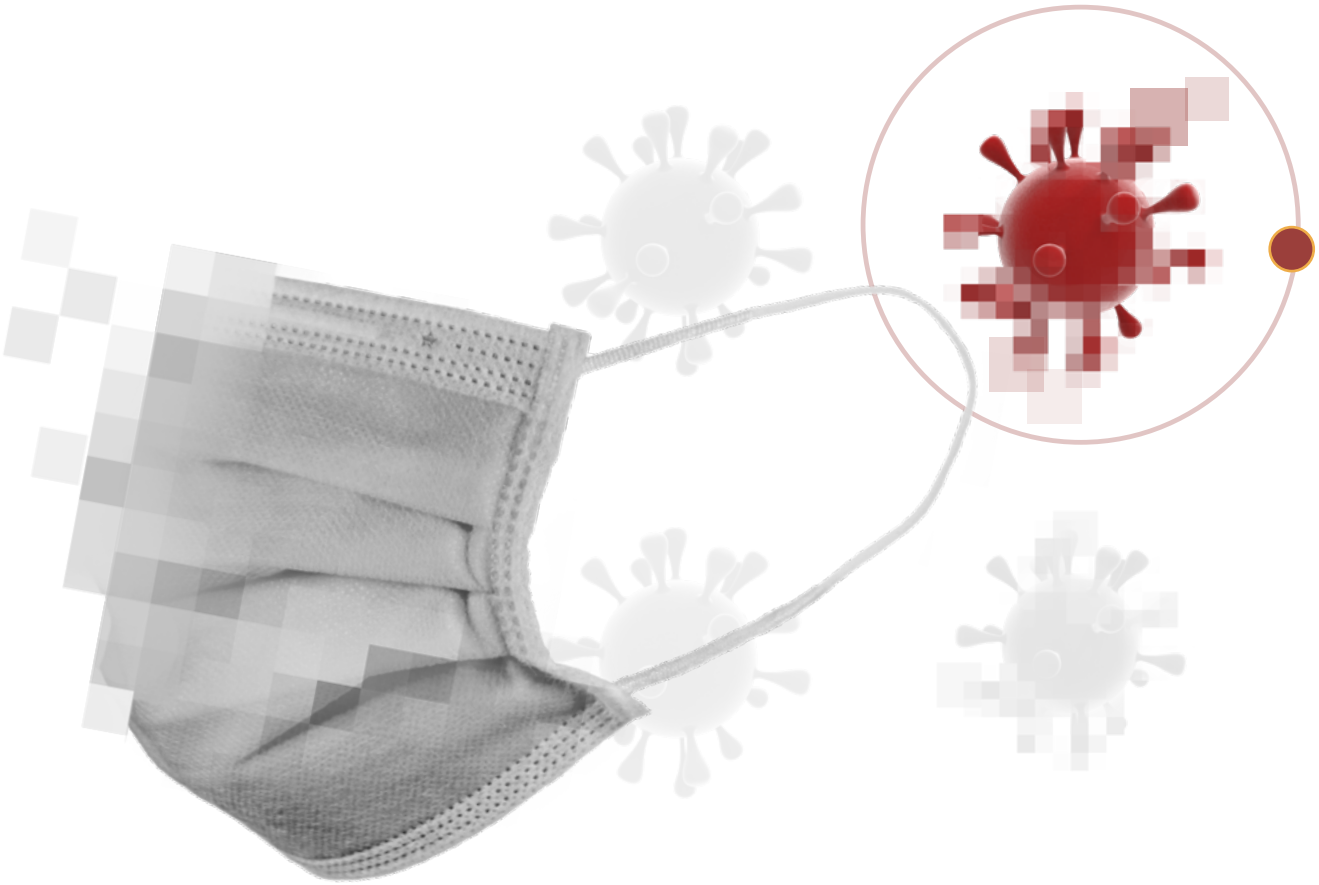
Patching is a critical control that nearly every insurer looks for. Software exploits can be avoided if software patches are up-to-date. They want to make sure that you are patching your systems, computers, applications, and software every week, especially if it is a high severity vulnerability. With remote work, many BYOD (bring your own device) or unmanaged devices are connecting to the network. It is important that these devices are patched and current on updates or they could be vulnerable to exploits.

Educating the Workforce

Unfortunately, humans are often an organization's weakest link. They are the ones clicking on a malicious link, sharing credentials and using poor password practices. Carriers like to see that you are keeping an educated workforce that understands the importance of security and their role in it.

There has been a shift towards zero trust and being more proactive about security resilience. MFA acts as the first zero trust layer of defense by mitigating risk, protecting credentials and preventing lateral movement. MFA and zero trust are an official recommendation from the White House's cybersecurity executive order, encouraging businesses to get on board. The National Institute of Standards and Technology (NIST) says "implementing a zero trust architecture has become a cybersecurity mandate and a business imperative."

Company IT teams are now far more involved in the process than they ever were before in meeting insurance requirements. It's hard to identify everything that drives pricing, but these controls are all critical to getting the best coverage. The more of these you have in place, the more carriers you will have interested in writing your coverage. This brings on more competition and allows your broker to negotiate and get the best pricing.



How the Pandemic Increased Attacks

The pandemic has changed the landscape for cyber insurance. Work is much broader now and goes beyond the brick-and-mortar office that everyone was commuting to five days a week. The move to remote work often creates more risk for companies. Today, ransomware is one of the biggest threats in cybersecurity, increasing by 150% during the COVID-19 pandemic due in large part to the sudden shift to remote work. This means that traditional firewalls and VPN connections are not necessarily indicators of trust. A zero trust approach to security assumes any access attempt might be a threat and needs to be validated before access is granted. Implementing zero trust by starting with MFA and device validation protects against credential stealing and exploits, keeping remote workers and applications protected.

What You Can Do to Prepare for Policy Renewal

Get ahead of your cyber liability insurance renewal by working closely with your IT team to implement the controls previously discussed. Review by mapping the risk surface and shoring up your security strategy. Strong practices can not only lower your premium but will also give you the strongest security stance possible. Have those conversations on what is feasible with the key stakeholders and decision-makers to understand the risk and options for your insurance needs versus asking your team to implement a new capability after a security product is purchased.

Discuss what new controls and procedures the insurance companies are going to ask for this year. Have a good inventory of your IT applications, users and devices. Who are your users? Where do they work? What applications and devices do they use? Document with resilience processes to review your security posture. Be prepared to review them against the list of items needed to shop liability insurance.

Not every standard insurer who offers cyber liability insurance can handle all the risks your company faces or provide adequate coverage. In these cases, a cyber security insurance broker can often step in to find specialized lines of coverage to meet the specific needs of each client. “Be sure your insurance broker is heavily marketing the account. All carriers are now asking for extremely substantial increases on renewals, and the way to get the best deal out there is if your broker is shopping around for you to multiple carriers in the marketplace. Be sure that the terms and conditions that you have at renewal are truly the best that’s available, because the terms and conditions vary more now than what they used to because of all the new policy changes happening,” Haney said. Make sure the policy terms reflect your business needs and will cover you in case of an incident.

How Duo Helps

Duo's multi-factor authentication is the foundation for good security hygiene and a zero trust architecture. Zero trust brings in elements of device trust and least-privileged access. We want to make sure that users are who they say they are, their device is trusted, healthy, up-to-date on patches and that they are given access to only what they need. Even if a bad actor gains credential access, the nature of zero trust is to check identification frequently and continuously with abnormal and irregular activity prompting higher security measures. With least privileged access, the user might not have had access to critical data in the first place if their role didn't need it. This not only protects breach of key information and networks, but also helps prevent lateral movement if one account is compromised.

Duo MFA, Duo Device Trust, Duo Network Gateway (DNG), Duo Single Sign-On (SSO), Duo Trust Monitor and Duo Device Health App combine into one trusted access solution that helps secure remote access to on-premises and cloud infrastructures, helping to prevent malware from easily getting access in the first place. Robust logging and reporting allows you to track who and what is accessing your applications and data.

Duo Protects With or Without a VPN

Malware can use remote services, such as Remote Desktop Protocol (RDP) and VPNs, to gain access to a network. The Duo Network Gateway (DNG) allows users to access on-premises websites, web applications, SSH servers and RDP, limiting access to the right users and devices. Duo Device Trust ensures that the device remotely accessing resources is a trusted computer and not an attacker's device. Duo Trust Monitor establishes a baseline and brings attention to authentication request anomalies that appear suspicious, such as those originating from countries where ransomware actors are known to be active, and countries where an organization does not have employees and continuously monitors for anomalies.

Common Insurance Requirements For Coverage

Validate users with MFA • Remote access to network • Remote Access to email • Privileged user access • Encrypted backups • Applications housing sensitive data • AWS, Azure and other servers	Duo MFA authenticates users at the application layer Duo Device Trust Identify risky devices, enforce contextual access policies, and report on device health Logging and reporting keeps a record of authentication attempts
Meet compliance requirements such as HIPAA, PCI-DSS, GDPR	Duo MFA for strong authentication Policies enforce device health requirements Duo Trusted Endpoints can limit access to corporate-owned devices Logging and reporting keeps a record of authentication attempts Adaptive Access Policies enforce user, device and location requirements at the application layer
Protect Remote Desktop Protocol (RDP)	Duo MFA for strong authentication Duo Device Trust Identify risky devices, enforce contextual access policies, and report on device health Duo Trusted Endpoints can limit access to corporate-owned devices Duo DNG (Duo Network Gateway) provides access to on-premises applications with RDP and enforces access requirements
Identify and address unusual behavior patterns	Trust Monitor identifies unusual login attempts based on individual users' typical behavior
Secure remote access for corporate users and vendors/contractors	Duo Trusted Endpoints can limit access to corporate-owned devices Duo DNG (Duo Network Gateway) provides access to on-premises applications without a VPN while also enforcing policies at the application layer. Reduces risk of lateral movement by ensuring users only have access to the applications they need
Keep devices updated and regular patching	Device Health App inspects computers and ensures device's operating system is up-to-date, password-protected, encrypted and firewall-enabled Adaptive Access Policies can prevent application access until updates are installed

Update Your Defense Beyond MFA With Duo

Organizations can defend against the impact of a breach through ransomware, social media and targeted phishing attacks by implementing conditional access policies that leverage contextual factors, such as location and the device posture, in order to establish user and device trust.

Duo's cloud-based security platform helps protect access to all applications, for any user and device, from anywhere. At Duo, we've simplified secure access to address identity and device risks with seven critical capabilities:

1. Verify users' identities with secure and flexible multi-factor authentication. Users can access applications at any time, from any device, for remote access anywhere.

2. Deliver a consistent login experience with Duo Single Sign-On, providing centralized access to both on-premises and cloud applications.

3. Gain visibility into every device, and maintain a detailed inventory of all devices that access corporate applications.

4. Establish device trust through health and posture checks for managed or unmanaged devices before granting application access. Duo helps you manage end of life software and update and maintain patches.

5. Enforce granular access policies to limit access to those users and devices that meet the organization's risk tolerance levels.

6. Monitor and detect risky login behavior using Duo Trust Monitor, or export logs to your SIEM, in order to remediate suspicious events such as new device enrollment for authentication or login from an unexpected location.

7. Duo Passwordless Authentication verifies a user's identity by easily allowing users to authenticate using biometrics, security keys or a mobile device.

Conclusion

Whether you are renewing your policy or getting cybersecurity liability insurance for the first time, you will likely face security requirements that must be met to get approval and the best rate. Ransomware has driven up the costs of cyber insurance due to its frequency and hefty price tag to remedy. To get ahead, there are some key controls almost every insurer looks for. Multi-factor authentication is the most important step to implement. Duo's multi-factor authentication and trusted access platform helps solve the MFA need of cyber insurance companies, and its protection helps build security resilience for your organization. It is a good idea to be prepared with fortified security hygiene practices in place before applying for or renewing cyber insurance to get the best coverage and rate.

Explore how Duo can uplevel your security posture and cyber insurance coverage.

Start a Free Trial

Duo Security, now part of Cisco, is the leading multi-factor authentication (MFA) and secure access provider. Duo is a trusted partner to more than 25,000 customers globally, including Bird, Facebook, Lyft, University of Michigan, Yelp, Zillow and more.

Try it for free at duo.com.

cisco SECURE

Cisco Secure delivers a streamlined, customer-centric approach to security that ensures it's easy to deploy, manage, and use. We help 100 percent of the Fortune 100 companies secure work – wherever it happens – with the broadest, most integrated platform.

Learn more at cisco.com/go/secure.